2020-06

SPECIAL OPERATIONS IN A 5G WORLD: CAN WE STILL HIDE IN THE SHADOWS?

Jones, Mason P.; McCaslin, Erica L.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**SPECIAL OPERATIONS IN A 5G WORLD:
CAN WE STILL HIDE IN THE SHADOWS?**

by

Mason P. Jones and Erica L. McCaslin

June 2020

Thesis Advisor:	Leo J. Blanken
Second Reader:	Justin P. Davis

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2020	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
SPECIAL OPERATIONS IN A 5G WORLD: CAN WE STILL HIDE IN THE SHADOWS?

5. FUNDING NUMBERS

6. AUTHOR(S) Mason P. Jones and Erica L. McCaslin

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Asymmetric Warfare Group, Fort Meade, MD 20755

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The arrival of "fifth generation" (5G) telecommunications technology is poised to fundamentally alter societies in numerous ways. Changes to telecommunications technologies and infrastructure will enable 5G networks to integrate information and collaborate at unprecedented levels, enabling leaps in artificial intelligence, human-machine teaming, and other data-based technologies. However, the thrill of emerging technologies and associated capabilities comes at a cost in terms of security vulnerabilities. Just as 5G will alter our daily lives, it will also modify our approach to Special Operations Forces (SOF) missions; bolstered by artificial intelligence, there is great potential for an adversary to aggregate and exploit data on a massive scale. Using qualitative evidence and deducing operational implications, this thesis develops a holistic framework of 5G networks, explores how this changing technological reality impacts signature management, and identifies the threats and opportunities within this domain. Ultimately, special operations forces will be forced to operate within high-risk telecommunications network environments, threatening their ability to sufficiently maintain operational security and manage their signatures. Near-term recommendations—data reduction and protection, force education, and network analysis during mission planning—and long-term research efforts—trusted communications, signature reduction, and deception techniques—may help mitigate these risks.

14. SUBJECT TERMS 5G, Special Operations Forces, SOF, signature management, operational security, deception, emerging technology, advertising technology, technical surveillance, China, Huawei	**15. NUMBER OF PAGES** 109
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

SPECIAL OPERATIONS IN A 5G WORLD: CAN WE STILL HIDE IN THE SHADOWS?

Mason P. Jones
Lieutenant Commander, United States Navy
BS, U.S. Air Force Academy, 2005

Erica L. McCaslin
Major, United States Air Force
BS, University of Washington, 2006
MBA, Trident University International, 2014

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)

from the

NAVAL POSTGRADUATE SCHOOL
June 2020

Approved by: Leo J. Blanken
Advisor

Justin P. Davis
Second Reader

Kalev I. Sepp
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The arrival of “fifth generation” (5G) telecommunications technology is poised to fundamentally alter societies in numerous ways. Changes to telecommunications technologies and infrastructure will enable 5G networks to integrate information and collaborate at unprecedented levels, enabling leaps in artificial intelligence, human-machine teaming, and other data-based technologies. However, the thrill of emerging technologies and associated capabilities comes at a cost in terms of security vulnerabilities. Just as 5G will alter our daily lives, it will also modify our approach to Special Operations Forces (SOF) missions; bolstered by artificial intelligence, there is great potential for an adversary to aggregate and exploit data on a massive scale. Using qualitative evidence and deducing operational implications, this thesis develops a holistic framework of 5G networks, explores how this changing technological reality impacts signature management, and identifies the threats and opportunities within this domain. Ultimately, special operations forces will be forced to operate within high-risk telecommunications network environments, threatening their ability to sufficiently maintain operational security and manage their signatures. Near-term recommendations—data reduction and protection, force education, and network analysis during mission planning—and long-term research efforts—trusted communications, signature reduction, and deception techniques—may help mitigate these risks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADTECH	Advertising Technology
AI	Artificial Intelligence
AR	Augmented Reality
ATAK	Android Tactical Assault Kit
BRI	Belt and Road Initiative
CCP	Chinese Communist Party
eMBB	Enhanced Mobile Broadband
GAN	Generative Adversarial Network
GPS	Global Positioning System
ICT	Information, Communication, and Technology
IoT	Internet of Things
mMIMO	Massive Multiple Input Multiple Output
mMTC	Massive Machine Type Communications
mmWave	Millimeter Wave Frequency
MSC	Mobile Switching Center
NFV	Network Functions Virtualization
OPSEC	Operational Security
RAN	Radio Access Network
RF	Radio Frequency
URLLC	Ultra-Reliable Low-Latency Communications
VR	Virtual Reality

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to acknowledge the mentorship, feedback, and guidance given by our dedicated thesis advising team, Dr. Leo Blanken and CDR Justin Davis. Their energetic style and dynamic partnership had a profoundly positive impact on our learning experience.

The "GOAT" in Asymmetric Warfare Group's N32 shop deserves a shout out for the support and sponsorship of this thesis project. Thank you to Mr. Dave Desrocher, LTC Scott Akerley, MAJ Eric Roles, CPT T.S. Allen, and Mr. Rocco Wecer for your outstanding support and feedback to our project.

Thank you to the entire Naval Postgraduate School faculty for their unyielding support and dedication to the higher learning of the officers and enlisted leaders of our United States military. We would especially like to thank Dr. John Arquilla, Dr. Alex Bordetsky, Dr. Doug Borer, Dr. Ray Buettner, CDR Clay Herring, Mr. George Lober, Dr. John Roth, Dr. Kalev Sepp, and Dr. John Tullius for their insights and exchange of ideas throughout this process.

Most importantly, the utmost thanks go to our families and friends who gave us the support and the time to pursue a thesis well outside the subject matter expertise of our chosen trades.

To my wife, thank you for the love and support to pursue this endeavor as a geographic bachelor. Thank you for your service to the Navy and our nation and for being a great mom to our son. I am forever in your debt.

To my husband, thank you for your mentorship, questioning mind, mindful attention, and playful humor during this academic adventure. I could have done this without you. *Not Even One Time…*

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The impact of "fifth generation" (5G) telecommunications technology is poised to fundamentally alter societies in several ways. When download speeds are boosted by a factor of one hundred, end-to-end latency is reduced to less than a millisecond, and network capacity is increased to support one hundred times the additional endpoint users and devices, we will see a new era in the digital age significantly impacting the way we communicate and how the world is connected.[1] Changes to telecommunications technologies and infrastructure will enable 5G networks to integrate and collaborate with information at unprecedented levels, enabling leaps and bounds in the use of artificial intelligence (AI), human-machine teaming, and other data-based technologies.

While a single "killer app" has yet to emerge, the applications powered by the expected data rates, the massive amount of connections, and edge computing will enable a range of use-cases that were previously theoretical. It may soon be commonplace for a doctor to remotely perform surgery from thousands of miles away, utilizing augmented reality informed by a healthcare database to diagnose and suggest a course of treatment.[2] The Internet-of-Things (IoT) will soon have the capacity and latency to support a metropolitan-level network of self-driving vehicles, altering the efficiency and safety of daily commutes. A hyper-enabled soldier may soon have real-time threat and intelligence analysis available on an Android/Tactical Assault Kit (ATAK)-enabled device, increasing force situational awareness and reducing time required to make mission-critical decisions. Despite the opportunities to enhance the warfighting abilities of our soldiers, the thrill of emerging technologies and associated capabilities comes at a cost. Each capability is paired with a specific signature that, if not properly managed, may put the end-user and their mission at significant risk.

---

[1] Patrick Agyapong et al., "Design Considerations for a 5G Network Architecture," *IEEE Communications Magazine* 52, no. 11 (November 2014): 4, https://doi.org/10.1109/MCOM.2014.6957145.

[2] Jennifer Alsever, "How 5G Will Fundamentally Change Everything You Know About Mobile Computing: From Farms to Phones," *Inc. Magazine*, February 2020, https://www.inc.com/magazine/202002/jennifer-alsever/5g-wireless-network-broadband-high-speed-gigabit-technology.html.

There are several ways in which the 5G world will be characterized by the IoT, geolocation, and the aggregation of individualized data. However, in our everyday lives, AI coupled with increasingly ubiquitous technical surveillance, mollified by the offer of convenience, is beginning to target individual consumers. The exploitation of this data within commerce is driven by advertising technology (ADTECH). In a 5G world, the potential for this practice to become more targeted is bolstered by the immense volumes of data coupled with extremely low latency and high bandwidth.[3] Though the analysis of a consumer's data in conjunction with their digital and physical signature may make their life more convenient, it also puts a consumer at risk of manipulation and exploitation. Take for example, a future 5G-enabled commute:

> After comparing her vital signs with historical data on a cloud-based network to determine an ideal wakeup time, Sally's Bluetooth-enabled smart watch initiates her alarm, optimizing her circadian rhythm while still ensuring she has adequate time for her typical morning routine. Her apartment, aided by the Internet-of-Things (IoT), streamlines her morning routine. Prior to her wakeup alarm, her watch conveniently adjusted the thermometer, started the coffee pot, and even fed her dog, Spark. Her refrigerator, noting that Sally is low on milk, frozen fruit, and her favorite, locally sourced avocados, seamlessly reorders these items in addition to the few grocery items she put on her virtual shopping list for tonight's dinner. After sipping her coffee, Sally hops into her network-connected shower, automatically set to a perfect 105-degrees, followed by a smart-mirror beauty routine, and steps out of her apartment to embark on her commute to work.
>
> As she leaves her apartment, the geolocation change of Sally's phone is registered by her apartment's security system. Knowing her typical routine, a self-driving car service is ordered, arriving just as Sally reaches

[3] Vandita Grover, "7 Ways 5G Will Help Advertising Evolve in 2019," *Martech Advisor* (blog), April 5, 2019, https://www.martechadvisor.com/articles/ads/7-ways-5g-advertising-evolve-2019/.

the curb. A camera connected to a facial recognition database confirms Sally's identity, charges the ride to her virtual account, and initiates her commute. Sensing that Sally is still feeling a little fatigued, her phone suggests a quick detour to visit her favorite café. Sally agrees and her vehicle is rerouted automatically.

Gig-a-Bites, wirelessly noting the approach of a regular customer and having purchased consumer data to include the spending habits of their patrons, not only prepares Sally's favorite soy matcha latte, but also cues the café screens to targeted advertisements aligned with her specific wants and desires. Sally finds her latte at the barista's counter and returns to her self-driving chariot. Bolstered by the efficiency and accuracy of the maintenance of her caffeine addiction, Sally's workday is off to a good start.

Sally arrives at *work* and finds her favorite park bench to set up for the day. Working remotely, Sally is able to access her cloud-based work server, gaining access to her email, video teleconferencing, and data processing applications. Enabled by a 5G network and edge computing, Sally, an industrial engineer and factory supervisor, ensures the machinery and processes in her factory are operating at peak efficiency, inspects the factory floor via augmented reality (AR), and makes wireless adjustments as required. From her sunny park bench, Sally is also able to access and monitor security patrols, although the partnered autonomous security system would notify both Sally and local security guards of any intrusion.

Upon completion of Sally's day, she decides to incorporate a workout into her commute. Sally is directed to the nearest ride-share bicycle, which automatically unlocks after registering Sally's digital signature, and she commences her ride home. On the way, the local grocer, having previously received her shopping request, is alerted to her pending arrival and is waiting outside with her order as she passes by. Enabled by the aggregation and analysis of her data, Sally's workday is complete.

Sally's story could easily continue with more examples of how a 5G world would enhance her day-to-day life; however, what is missing from this narrative are the sacrifices in privacy and security that Sally made to enjoy these conveniences.[4]

While proposed 5G infrastructures have some inherent security built in, much of data security, and therefore signature management, will still depend on the individual user. Just as 5G will alter the way we go about our daily personal lives, it will necessarily change our approach to special operations forces (SOF) missions, whether on or off the battlefield. Both societies and militaries have grown addicted to technology while the lines between war, conflict, competition, and peace continue to blur.[5] It is unrealistic to think that individuals or entire units can remain concealed as they once were. The implications of an opponent's capacity to aggregate and utilize personal data and metadata on a massive scale is worth investigating. Will it be possible for an adversary in the future to overcome our operational security and anticipate combat operations by weaponizing advertising technology? With that question in mind, this thesis aims to provide a foundational understanding of the proposed 5G infrastructure and capabilities, the proliferation of these networks by our adversaries, an appreciation for how this changing technological reality might impact signature management as well as to recognize threats and opportunities within this domain.

A. PURPOSE

To prepare our forces and maintain the competitive advantage during future conflicts, it is important to understand the impact of emerging technologies upon special operations. The U.S. military often approaches most problems with a reliance on faster innovation—until recently, this confidence in advanced technologies has preserved the advantage the United States enjoys over her adversaries and their proxies. The last two

---

[4] Shoshana Zuboff, "You Are Now Remotely Controlled," *The New York Times*, January 24, 2020, sec. Opinion, https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

[5] Steven Bryant, "The Dangers of an Over-Reliance on Technology" (master's thesis, Norfolk, VA, Joint Advanced Warfighting School, 2011), 1–3; Sergio Miracola, "Chinese Hybrid Warfare," *Italian Institute for International Political Studies*, December 21, 2018, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853.

decades of conflict against non-state actors around the world has solidified these assumptions within our doctrine. However, as a result of this technological asymmetry, our forces have a near-complete reliance on Global Positioning System (GPS) navigation, communications systems that rely on robust infrastructure, weapons systems dependent on a large logistical footprint, and have grown accustomed to the normal emissions of uniquely U.S. military signatures.[6] This approach may be significantly challenged by a more sophisticated adversary and it is likely that the United States and her allies have atrophied in their ability to fight a technological peer.[7] Anticipating a nexus between great power competition, 5G telecommunication technology, and advanced artificial intelligence, this thesis will seek to offer implications of operating within an environment proliferated with 5G technology. While this thesis will remain largely descriptive, we will also strive to provide recommendations for future research to assist SOF operations, highlighting the gap between our current capabilities and the rapidly evolving technological environment.

B. RESEARCH QUESTIONS

As the technological reality changes for our forces on the battlefield, several research questions have emerged relative to the impact of next generation telecommunications technology on SOF operations. Key questions this thesis will explore are:

- What are the implications of 5G technology for signature management?
- Can special operations forces employ deception tactics in concert with signature management to mitigate operational and tactical risks posed by advanced telecommunications networks?
- What are the implications of the rapid fielding of 5G in the developing world?

[6] Bryant, "The Dangers of an Over-Reliance on Technology," 22–24, 29–30.

[7] Keven P Coyle, "U.S. Military Technology Dependence: The Hidden Vulnerability to National Security" (master's thesis, Norfolk, VA, Joint Advanced Warfighting School, 2016), 1–3; Bryant, "The Dangers of an Over-Reliance on Technology," 1–3.

- Within the 5G environment, can special operations forces manage their physical and digital signatures?
- What further research and analysis is required to ensure the United States adequately applies sound signature management strategies within a 5G environment?

C. APPROACH

Using qualitative evidence and deducing operational implications from current and projected 5G technical characteristics, this thesis will focus on developing a holistic framework of 5G networks for the SOF operator. Ubiquitous technical surveillance and advertising technology-based threats will serve as the backdrop of threats assessed throughout this thesis; however, in the context of changing technological realities, principles of signature management and deception will be used to focus recommendations into avenues for further research relevant to small unit teams.

D. ORGANIZATION

Organized into five chapters, this thesis will begin with an introduction into the 5G world and end with specific implications of this emerging technological reality and specific recommendations. Chapter II surveys 5G networks and capabilities, providing the technical framework needed for SOF operators and decision-makers to apply signature management within operational planning and assessment. Chapter III will look specifically at the Chinese "Digital Silk Road" strategy and their rapid proliferation of 5G technology, providing multiple vignettes showcasing the implications of Chinese 5G expansion.[8] Chapter IV begins with a discussion of signatures, signature management, and the role of deception to manage information. A hypothetical special operations vignette illustrates the challenges 5G technology presents to signature management and sets the stage for a discussion of the overall implications. After distilling the previous discussions into a threat model, the final chapter will offer recommendations and future research opportunities.

[8] Yash Mishra, "Here Are the Countries That Allowed Huawei to Build 5G," *Huawei Central* (blog), August 30, 2019, https://www.huaweicentral.com/here-are-the-countries-that-allowed-huawei-to-build-5g-list/.

II. A SURVEY OF FIFTH GENERATION (5G) TELECOMMUNICATION TECHNOLOGY

> The 5G world will be a collaborative ecosystem, and the role of what each of us will do in that remains to be thought through.[9]
>
> —Borje Ekholm, CEO Ericsson

As fifth generation (5G) networks and associated technologies begin to emerge this year, the final framework is still undetermined. This type of progressive roll out is not abnormal in the development of next generation telecommunications technology; as the developmental process unfolds, the standards evolve from theoretical to practical, often based on operational testing, infrastructure and market limitations, and advances and constraints of the technology. What is known, however, is that the emergence of 5G capabilities will have dramatic impacts on civilian and military operations alike. The traditional divide between civilian and military technological capabilities will become blurred and opportunities within the civilian sector may also present threats within the defense sector. To better understand these opportunities and threats, this chapter will explore the evolution and fundamentals of mobile wireless technology, the technology supporting the 5G framework, and the end-user devices and capabilities that industry is striving for. Along the way, we will highlight key differences from the existing 3G/4G LTE network, however, an assessment of the implications and recommendations will be reserved for later chapters.

A. EVOLUTION OF MOBILE WIRELESS TECHNOLOGY

Mobile wireless technology has changed the way the world is connected. Though its evolution has been steady since the 1970s, the impact of this technology has had varied and far-reaching impacts on the world. Not only has mobile wireless technology altered telecommunications, it has fundamentally changed the way the world interacts socially, the

9 "Ericsson Sees Light in Tunnel," *The Australian Business Review*, March 17, 2017, https://www.theaustralian.com.au/business/technology/ericsson-sees-light-at-end-of-tunnel-thanks-to-telstra-tieup/news-story/d1971a894cb2d1990d3dd29f3b0203ac.

speed at which information is exchanged, and the nature of commerce. Once again, the next generation promises to expand the impact telecommunications has on the world; however, in addition to building on existing capabilities, 5G will make some fundamental changes to the wireless networking framework. Figure 1 quickly sums up the additive capabilities that were adapted in each successive generation.

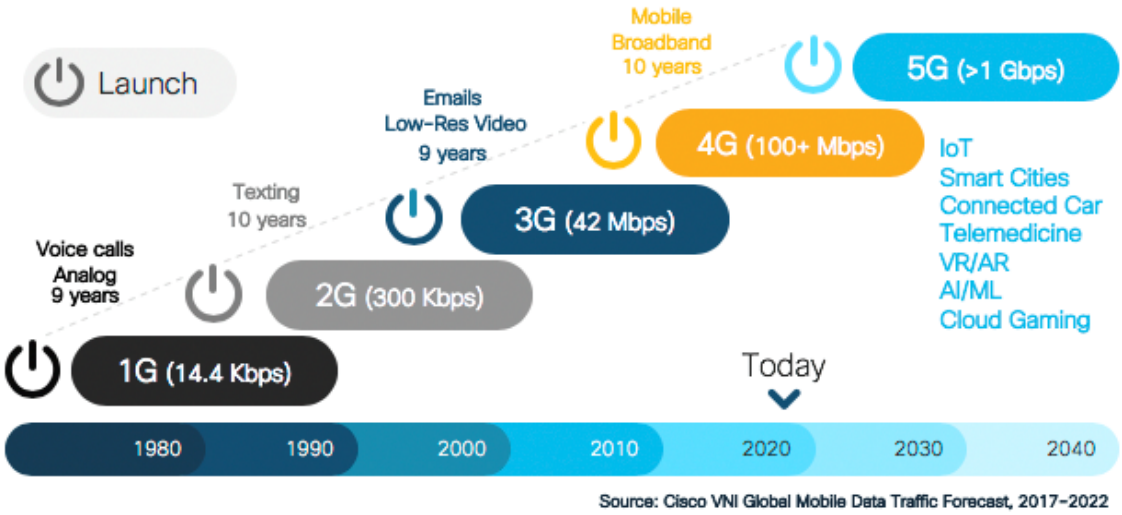


Figure 1. Cellular Technology Evolution[10]

1G. Development of cellular networks and mobile wireless technology began in the 1970s and debuted in the 1980s.[11] While first generation (1G) technology lacked the sophistication and security of the today's frameworks, the ability to transmit data on a radio network was groundbreaking.[12] Gupta and Jha describe these networks in their IEEE 5G Survey as vulnerable, unreliable, and lacking the necessary capacity; data transmission peaked at 2.4kbps, supporting voice calls (and limited data transfer) which were vulnerable

[10] Source: Shruti Jain, "Mobile VNI Forecast 2017–2022: 5G Emerges and Is Here to Stay!!," *Cisco Blogs* (blog), February 26, 2019, https://blogs.cisco.com/sp/mobile-vni-forecast-2017-2022-5g-emerges.

[11] Sunny Classroom, "5G Cellular Networks: 6 New Technologies," https://www.youtube.com/watch?v=hQvHNVRv_ms; A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access* 3 (2015): 1207, https://doi.org/10.1109/ACCESS.2015.2461602.

[12] Gupta and Jha, "A Survey of 5G Network," 1207; Milo Medin and Gilman Louie, *The 5G Ecosystem: Risks & Opportunities for DOD* (Defense Innovation Board, 2019), 5.

to third-party interception.[13] Medin and Louie further distinguish the system by its analog "hand-offs" via a distributed network of base stations.[14]

2G. The 1990s saw wireless technology improve in its second generation (2G) with the introduction of digital technology.[15] Data rates improved dramatically (up to 200kbps in later iterations of 2G) and the standard introduced rudimentary digital encryption.[16] End-users gained additional capabilities including Short Message Service (SMS) and email.[17]

3G. The 2000s ushered in the third generation (3G) of cellular networking, merging internet protocol (IP) services with mobile access and supporting initial data transfer rates up to 2Mbps.[18] The inclusion of data packet-switching enabled video calling, data streaming, and internet access. Current 3G networks have increased data rates up to 1Gbps.[19] During this time, the Third Generation Partnership Project (3GPP) collaborated on common standards for 3G networks and end-user technology to align worldwide compatibility.[20] This international partnership continues throughout 4G/LTE standards as well as the current efforts to develop 5G.

4G/LTE. Fourth generation (4G)/Long-term Evolution technology (LTE) enabled complete reliance on IP, a ten-fold improvement in data transfer rate, and a mobile networking experience comparable to Wi-Fi or traditional internet connections (services include Digital Video Broadcasting, video chat, and mobile TV).[21]

---

[13] Gupta and Jha, "A Survey of 5G Network," 1207.

[14] Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD,* 5.

[15] Gupta and Jha, "A Survey of 5G Network," 1207.

[16] Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD,* 5.

[17] Gupta and Jha, "A Survey of 5G Network," 1207.

[18] Gupta and Jha, 1207.

[19] Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD,* 5

[20] Medin and Louie, 16.

[21] Gupta and Jha, 1208; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD,* 5–6.

5G. As the 3GPP continues to deliberate on the future standards for fifth generation (5G) cellular networks, the eventual architecture of 5G is yet to be determined. However, there are several capability challenges that the industry agrees that 5G should meet; these capabilities will "enable enhanced mobile broadband (eMBB), massive internet of things (IoT) or massive machine type communications (mMTC), and ultra-high reliable and low latency communications (URLLC) services."[22] Major adaptations that will enable these services include massive multiple input multiple output (mMIMO), or the ability to connect an extraordinary number of devices, and the utilization of millimeter waves (mmWaves) that will introduce untapped bandwidth and dramatically increase network data rates.[23]

B. 5G ADVANCEMENTS

The transition to 5G could fundamentally advance consumer, industry, and military applications, altering the way we work, play, and integrate with our environment. Dramatic increases in the number of connections, enhanced network capacity, and ultra-low latency are three primary capabilities that will be enriched by this next generation technology; however, this will not be possible without significant changes to technology and infrastructure. Common among a few works, there are four challenges or criteria that are generally accepted by industry leaders and developers to meet the threshold of next generation (5G) telecommunication technology as well as relevant to our signature management discussion.[24] These include:

- **Massive number of connections (x10-100)**

[22] Gordon J. Sutton et al., "Enabling Technologies for Ultra-Reliable and Low Latency Communications: From PHY and MAC Layer Perspectives," *IEEE Communications Surveys Tutorials* 21, no. 3 (Third Quarter 2019): 2488, https://doi.org/10.1109/COMST.2019.2897800; Agyapong et al., "Design Considerations for a 5G Network Architecture," 4; "Public Policy Position: 5G Spectrum" (Huawei, 2017), 6, https://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_position_5g_spectrum.pdf.

[23] Agyapong et al., "Design Considerations for a 5G Network Architecture," 4; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 9–10.

[24] Agyapong et al., "Design Considerations for a 5G Network Architecture," 4.

Cellular IoT devices (e.g., wearable devices, smart home appliances, autonomous vehicles, sensors, and so on) are estimated to reach 3.5 billion worldwide by 2023, increasing from 700 million in 2017.[25] Estimates predict that the cumulative architecture, frequency, and antenna advancements of 5G will allow the network to grow from 1000 connections/km^2 to over a million connections/km^2.[26]

- **Bandwidth (Rate increase x10)**

  Bandwidth, which is directly related to data rates, suggests the volume of data transferred in a unit of time, generally measured in bits per second. Data consumption is exponentially increasing worldwide; 3G/4G networks expect data usage to increase from 20 exabytes in 2018 to over 80 exabytes by 2023.[27] 5G networks may meet these demands by utilizing greater frequency bands within the largely untapped high-frequency range. Doing so will provide 1~10 Gbps data rates for the densely populated massive number of connections; this represents at least a nearly ten-fold increase in speed compared to LTE's 150 Mbps peak rate.[28]

- **Latency (<1ms Roundtrip)**

---

[25] Agyapong et al., 2; "Ericsson Mobility Report" (Stockholm, Sweden: Ericsson, June 2018), 16, https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf.

[26] Agyapong et al., "Design Considerations for a 5G Network Architecture," 4; "Difference Between 4G and 5G," accessed February 7, 2020, https://www.rfwireless-world.com/Terminology/4G-vs-5G-difference-between-4G-and-5G.html; Mamta Agiwal, Navrati Saxena, and Abhishek Roy, "Towards Connected Living: 5G Enabled Internet of Things (IoT)," *IETE Technical Review* 36, no. 2 (March 4, 2019): 196, https://doi.org/10.1080/02564602.2018.1444516; Mamta Agiwal, Abhishek Roy, and Navrati Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 1618.

[27] "Ericsson Mobility Report," 14.

[28] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1618.

Latency, generally measured in milliseconds, represents the time required for data to travel from the source to its destination and back. Reducing LTE's top latency by ten-fold, 5G networks will see 1ms roundtrip latency.[29] Enabling emerging technologies that require almost immediate feedback, such as autonomous vehicle-to-vehicle (V2V) communication or battlefield surgery via augmented or virtual reality, latency of less than 1ms is critical to near real-time applications within 5G networks.[30]

- **Quality of Experience**

  Extremely low latency, high bandwidth, traffic optimization techniques, and at-the-edge computing are 5G characteristics that promise an improved and more consistent quality of experience.[31] To provide the necessary quality, intelligent network optimization will push more resources (bandwidth, latency, etc.) to demanding applications such as video streaming or augmented reality; other, less demanding applications such as the internet-of-things (IoT) will be allocated fewer resources.[32] From the end-user, success is defined to be when perceived availability is 99.999% and coverage extends to 100% of user locations.[33]

C. FUNDAMENTAL TECHNOLOGICAL CHANGES

To achieve these important criteria, there are several required upgrades or additions to the existing infrastructure as well as needed scientific research to develop, test, and implement the technology. The allocation of new radio wavelength bands, alterations to the cellular base station architecture and network control, as well as the design of smart

---

[29] Agiwal, Roy, and Saxena, 1618.

[30] Agyapong et al., "Design Considerations for a 5G Network Architecture," 5; Kimberly Underwood, "5G for Warfighters," *SIGNAL Magazine*, June 1, 2019, https://www.afcea.org/content/5g-warfighters.

[31] Agyapong et al., "Design Considerations for a 5G Network Architecture," 7.

[32] Agyapong et al., 7.

[33] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1618.

and directional antennas are only a few of the technical challenges 5G innovators will face. The Appendix provides a more in-depth discussion of these developments; however, the remainder of this section will strive to provide a brief overview.

1. Wavelength Bands

As more wireless technology is added to the network, the already overcrowded frequency bands risk reducing the overall network capability and quality of experience. In response, scientists and industry leaders are exploring other frequency bands in addition to techniques for more efficient use of current bands. Distinctive low, medium, and high bands are under examination, each offering unique opportunities and drawbacks (Figure 2).[34]

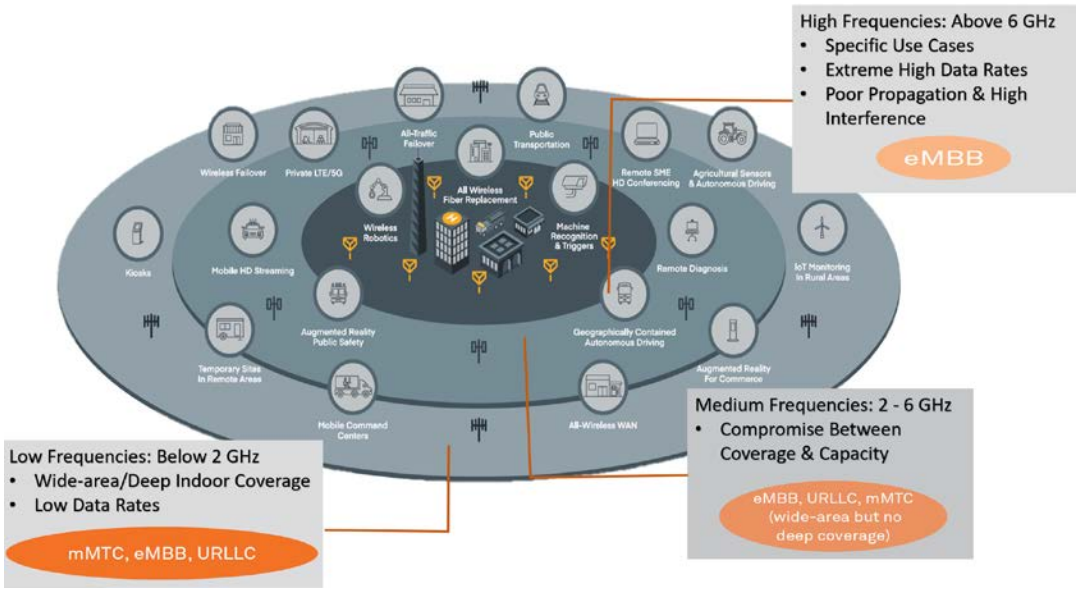


Figure 2. Multi-Layer Frequency Overlay on 5G Use-Cases[35]

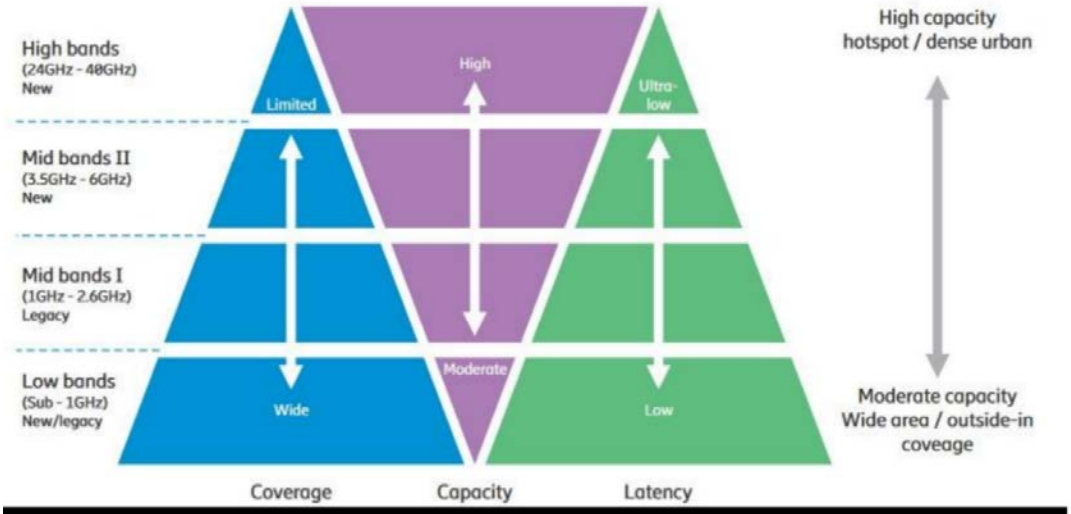
While the majority of our telecommunication currently occurs within the low wavelength bands (3kHz–3GHz), the authors of the 5G telecommunication standards are

---

[34] "Public Policy Position: 5G Spectrum," 6; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 12.

[35] Adapted from "Public Policy Position: 5G Spectrum," 6; Cradlepoint 5G Strategy Group, *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*, 2nd ed. (Boise, ID: Cradlepoint, 2020), 7–8, www.cradlepoint.com/5G.

primarily assessing the less-crowded medium and high bands for enhanced mobile broadband.[36] This will allow a simultaneous transition of less bandwidth-demanding technology to the crowded lower bands (e.g., IoT devices that require low data rates).[37] Currently, there is some debate over which of the wavelength bands will offer the most promise for mobile broadband; the United States continues to pursue the highest, mmWave bands (>24GHz) while other nations, such as China, have begun to implement within the sub-6 bands (3-6GHz).[38] The trade-offs associated with each band are summarized in Figure 3; balancing capacity and latency with wide-area coverage and building penetrations will require a blend of each band.[39]



5G spectrum trade-offs (Source: IEEE).

36 "Radio-Frequency Spectrum," in *Encyclopedia Britannica*, 2013, https://www.britannica.com/science/radio-frequency-spectrum; Cradlepoint 5G Strategy Group, *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*, 7; Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1618.

37 "Radio-Frequency Spectrum"; Cradlepoint 5G Strategy Group, *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*, 7.

38 Sunny Classroom, "5G Cellular Networks"; "Public Policy Position: 5G Spectrum," 10; Anne Morris, "Ericsson Hails 5G Test on Another Sub-6 GHz Band," *SDxCentral*, January 14, 2019, https://www.sdxcentral.com/articles/news/ericsson-hails-5g-test-on-another-sub-6-ghz-band/2019/01/; T-Mobile, "Built for the 5G Future: T-Mobile Opens New Device Lab," August 20, 2019, https://www.t-mobile.com/news/5g-device-lab.

39 Paula Gilbert, "Spectrum for 5G Will Ensure Investment in Africa," *ITWeb*, November 20, 2018, sec. Telecom, https://www.itweb.co.za/content/dgp45qaGWaD7X9l8.

Figure 3. 5G Spectrum Trade-Offs[40]

2. Network Architecture

The current radio access network architecture is largely base station centric with systematically placed macro base stations.[41] However, the higher frequency bands identified for 5G telecommunication will require a much denser architecture of base stations as well as a massive number of cells and antennae; this network design will help overcome the low propagation and high interference characteristics of the medium and high bands.[42] This architecture will range from macro-cells for wide-area coverage down to femto-cell deployments for dense urban coverage.[43] However, it is this architecture that will provide massive amounts of data and ultra-low latency to an incredible number of devices.[44]

3. Changes to Antenna Technology

The shorter, high frequency waves proposed for the medium and high bands will require closer, line-of-sight signals to maintain a connection.[45] Although the negative wave characteristics drive a dense network architecture, this dense layout of antennae combined with massive multiple input multiple output (mMIMO) technology and nimble antenna pathways to maintain adequate line-of-sight signal strength (e.g., spatial diversity, multiplexing, and beamforming) will ensure the immense number of connections are supported.[46]

---

[40] Source: Gilbert.

[41] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1620.

[42] Agiwal, Roy, and Saxena, 1621.

[43] Agiwal, Roy, and Saxena, 1621.

[44] Agyapong et al., "Design Considerations for a 5G Network Architecture," 4–5; Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1627.

[45] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1621.

[46] Agiwal, Roy, and Saxena, 1621; Qualcomm, "How 5G Massive MIMO Transforms Your Mobile Experiences," June 20, 2019, https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences.

D. 5G IN ACTION

Depending on your perspective, 5G may mean something completely different to you than it does to your neighbor. For some, 5G means greater bandwidth. For others, it provides ultra-low latency. And for a different group, it connects a massive number of devices to the network. However, when these characteristics are combined, some very interesting capabilities and applications are enabled (Figure 4).[47] Self-driving cars, industrial automation and other mission-critical systems will rely on ultra-reliable low-latency communications (URLLC).[48] Integrated sensors, security cameras, and machine-type communications will depend on massive connectivity and the IoT.[49] Finally, enhanced mobile broadband will enable data transfer rates in the 1Gbps range, allowing for an incredible amount of data to be transferred, aggregated, and processed in near real-time.[50]

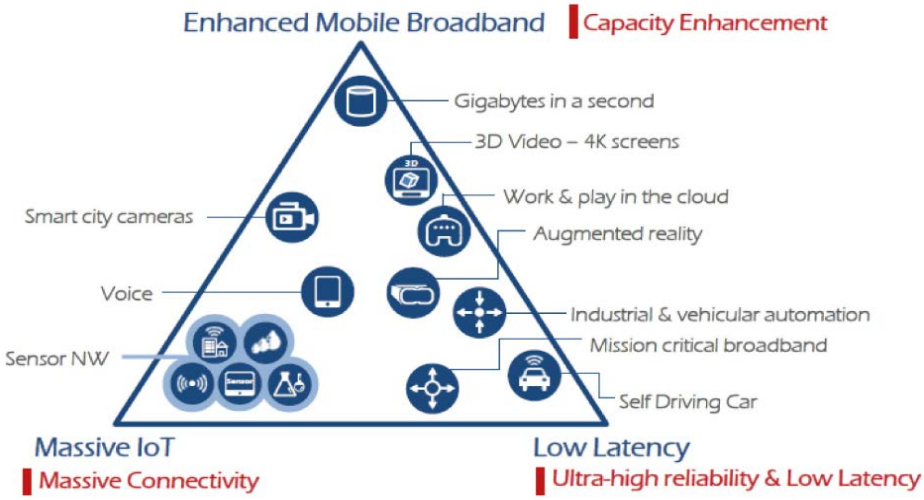


Figure 4. 5G Capabilities and Use Cases[51]

47 "Standards," 2020, https://futurenetworks.ieee.org/standards.

48 IEEE Future Networks: Enabling 5G and Beyond.

49 IEEE Future Networks: Enabling 5G and Beyond; Agiwal, Saxena, and Roy, "Towards Connected Living: 5G Enabled Internet of Things (IoT)," 191.

50 IEEE Future Networks: Enabling 5G and Beyond, "Standards"; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 9.

51 Source: IEEE Future Networks: Enabling 5G and Beyond, "Standards."

Though the standards are still being determined, the industry has generally agreed on the capability requirements and have begun to move forward on implementation. Already, 5G is available in several cities worldwide as providers as well as their state-sponsors continue to compete in the telecommunications domain.[52] As 5G proliferates around the world, devices and applications will soon follow; applications such as augmented reality, smart cities, and industrial automation that have stalled under the current telecommunications regime will be more empowered and capable as more robust 5G networks are realized.[53]

Much of the discussion relative to capabilities and applications is driven, not surprisingly, by civilian demand and industry. However, many of these same capabilities can be adapted for military applications. If integrated with artificial intelligence (AI) or machine automation, intelligence collection and analysis could be done at the edge on the battlefield.[54] Enabled by enhanced mobile broadband and ultra-reliable low-latency battlefield capabilities, soldiers could clear an ISIS-controlled neighborhood aided by augmented reality, reducing the risk to themselves and civilians. Autonomous intelligence, surveillance, and reconnaissance drones could perform real-time route reconnaissance and alert the team of impending threats. However, 5G may also enable adversarial threats that may risk the signature management of a special operations team; ubiquitous technical surveillance and AI-supported advertising technology-enabled targeting may hinder a SOF team's ability to protect their signature and operational security.

---

[52] Sascha Segan, "T-Mobile Announces 5G in 6 Cities: We Have the Maps," *PCMagazine*, June 25, 2019, https://www.pcmag.com/news/t-mobile-announces-5g-in-6-cities-we-have-the-maps; Eli Blumenthal, "AT&T Bolsters 5G Network with New Low-Band and Millimeter-Wave Markets," *CNET*, December 30, 2019, https://www.cnet.com/news/at-t-bolsters-5g-network-with-new-low-band-and-millimeter-wave-markets/.

[53] "5G & the Future of Connectivity: 20 Industries the Tech Could Transform," March 19, 2019, https://www.cbinsights.com/research/5g-technology-disrupting-industries/.

[54] Manlio Dinucci, "The Hidden Military Use of 5G Technology," *Telesurtv*, December 21, 2019, sec. Opinion, https://www.telesurenglish.net/opinion/The-Hidden-Military-Use-of-5G-Technology-20191221-0006.html.

1. Technical Surveillance

Technical surveillance is nothing new to militaries, police, or intelligence agencies. Security cameras, voice and data collection, spectrum analysis, and various remote sensors have enabled surveillance and collection for decades. However, in a 5G regime, this type of surveillance will become more ubiquitous and inexpensively proliferated to state and non-state actors.[55] At the most basic level, commercially available, benign hardware and software is easily accessible and the capabilities are adaptable for use by criminal and non-state actors.[56] At the high end of state-controlled technical surveillance, collection and analysis is deeply integrated and supported by a well-established organization to operationalize the data and intelligence gained.[57]

While there is a bit more inherent security built into the network to protect end-to-end information, the sheer number of devices connected to the network may introduce new risks to operations within an untrusted 5G network. As 5G is adopted, the ability to surveil the general populace as well as adversaries will grow. Geolocation, facial recognition, device metadata, and personal data remain vulnerable to collection and exploitation.[58] Surveillance states have already begun to monitor the most mundane actions of its citizens and implement the infrastructure and policies required to ensure there are no blind spots in the future.[59] 5G technology, due to the increased volume and speed at which data is

---

[55] Steven Feldstein, "The Global Expansion of AI Surveillance" (Washington, DC: Carnegie Endowment for International Peace, September 17, 2019), 1–3, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847; Niraj Chokshi, "How Surveillance Cameras Could Be Weaponized with A.I.," *The New York Times*, June 13, 2019, sec. U.S., https://www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html.

[56] Feldstein, "The Global Expansion of AI Surveillance"; Chokshi, "How Surveillance Cameras Could Be Weaponized with A.I."

[57] Feldstein, "The Global Expansion of AI Surveillance"; Dinucci, "The Hidden Military Use of 5G Technology."

[58] Feldstein, "The Global Expansion of AI Surveillance," 1–2,10.

[59] Nicholas Wright, "How Artificial Intelligence Will Reshape the Global Order," October 11, 2019, https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

transmitted and analyzed, as well as changes to behavioral norms, decreasing the privacy of the individual, may enable greater surveillance and control of populations in the future.

This type of technical surveillance, enhanced by a 5G network, has impacts to signature management in the physical, electromagnetic, and behavioral domains. It will be possible, more than ever, to develop individual, actionable profiles from the collected data. In the commercial sector, this type of data is valuable to advertising and marketing firms; in fact, much of this type of data is already actionable against consumers in the form of contextual marketing powered by advertising technology (ADTECH).[60]

2. Contextual Marketing Facilitated by AI-enabled ADTECH

Though the military implications of ADTECH will be explored in follow-on chapters, a discussion of this technology in the civilian context will inform an understanding of how it may be weaponized in the future. Massive amounts of personal data, often freely given, are available to advertising and marketing firms and have changed the way industry engages with consumers. As 5G supports a more robust IoT, the amount and variety of data available to industry will grow, enabling personalized, contextualized, real-time marketing.[61] Figure 5 highlights the relationship between IoT-derived personal information (i.e., geolocation, biometrics, etc.), environmental data, and behavioral preferences; through artificial intelligence, human-machine teaming, and the data marketplace, this information is bought, sold, distilled, and actioned upon in near real-time.[62]

---

[60] Thomas Husson, "Mobile's Untapped Value Is in Contextual Data," *Forrester* (blog), October 27, 2014, https://go.forrester.com/blogs/14-10-27-mobiles_untapped_value_is_in_contextual_data/.

[61] Husson; Mathew Broughton, "The Future Is 5G: How New Mobile Tech Will Take Advertising into the 5th Generation," *Exchange Wire* (blog), April 29, 2019, https://www.exchangewire.com/blog/2019/04/29/the-future-is-5g-how-new-mobile-tech-will-take-advertising-into-a-fifth-dimension/; Grover, "7 Ways 5G Will Help Advertising Evolve in 2019."

[62] Husson, "Mobile's Untapped Value Is in Contextual Data."

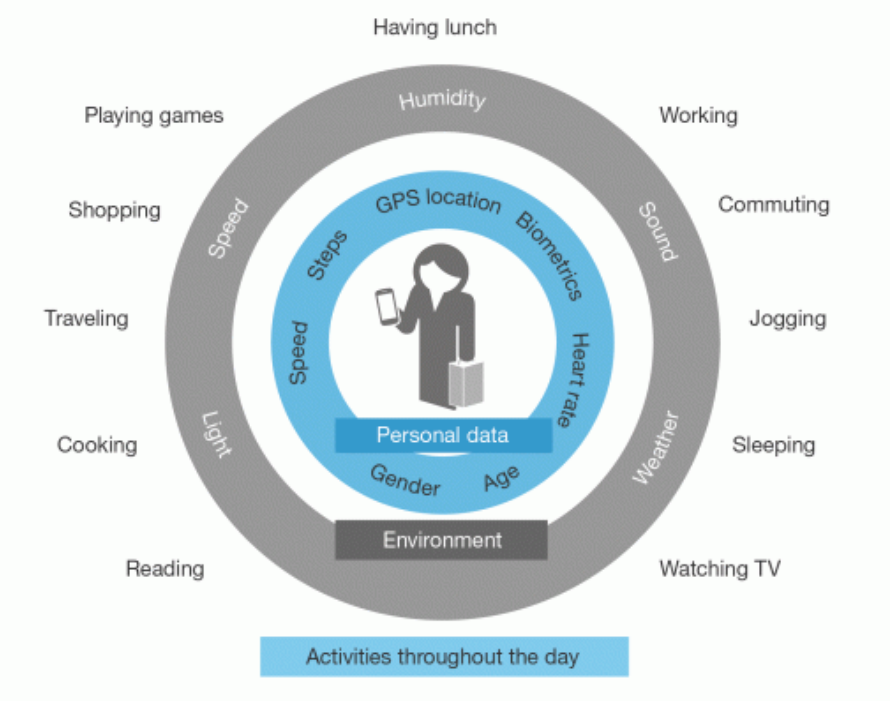


Figure 5. Data Utilized for Contextual Marketing[63]

Google ads, refined by a user's search history, are an early example of contextual marketing. However, as technology advances and behavioral norms adapt (i.e., privacy concerns are often ignored for convenience or participation in the online marketplace), the power of AI-enabled ADTECH will continue to drive growth in contextual marketing or, as Shoshana Zuboff refers to it, surveillance capitalism.[64] Advancements in next generation telecommunications will allow for targeted messaging via augmented reality, high-speed 4K video advertising, and personalized ads on a range of IoT-connected devices.[65] However, beyond the immediate interactions, AI-enabled ADTECH can anticipate consumer preferences, predict future behavior, and inject interactions based on this analysis.[66]

---

[63] Source: Husson.

[64] Husson; Shoshana Zuboff, "'Surveillance Capitalism' Has Gone Rogue. We Must Curb Its Excesses," *The Washington Post*, January 24, 2019, sec. Opinion.

[65] Grover, "7 Ways 5G Will Help Advertising Evolve in 2019."

[66] Husson, "Mobile's Untapped Value Is in Contextual Data."

ADTECH, ultimately, is enabled by the data end-users provide—often unknowingly—to the algorithms. Personal preferences, patterns of life, geolocation, and other metadata is utilized by ADTECH to synthesize personal profiles of each consumer. Generally, this data is anonymized, yet there are ample opportunities to still exploit users. The entire online advertising ecosystem connects consumers to advertisers and publishers via ad platforms and data aggregators. The aggregators are systems that collect enormous amounts of user data with "the specific aim of profiling their interests."[67] Through a variety of tools to include first and third party tracking, cookies, cookie matching technology, and device fingerprinting, these aggregators have designed data mining techniques that may even overcome moderate data protection best practices.

First-Party Tracking. In this form of online tracking, the websites (i.e., ad publishers) allow data aggregation of the end-users. The consumer data is collected through HTTP cookies (a packet of information logging historical web traffic) and cookie monitoring as well as cataloguing information directly entered by the user.[68] Generally, first-party tracking is unique to a specific domain.

Third-Party Tracking. Similar to first-party tracking, these tools use indirect means to monitor and gather internet user information via an intermediary not specifically tied to a domain.[69] This activity usually occurs unbeknownst to individuals utilizing the internet and can lead to "massive aggregation of personal information."[70]

Cookie-Matching Technology. Cookie matching enables aggregators to share cookies or a collection of cookies with numerous advertisers or demand-side platforms. The effect of this technology allows advertisers a more holistic look at

---

[67] José Estrada-Jiménez et al., "Online Advertising: Analysis of Privacy Threats and Protection Approaches," *Computer Communications* 100 (March 1, 2017): 35, https://doi.org/10.1016/j.comcom.2016.12.016.

[68] "What Are Cookies?," Norton, 2020, https://us.norton.com/internetsecurity-how-to-what-are-cookies.html; Estrada-Jiménez et al., "Online Advertising," 38.

[69] Estrada-Jiménez et al., "Online Advertising," 38.

[70] Estrada-Jiménez et al., 38.

an end-user's previous online habits and the ability to filter out consumers who do not match a predetermined profile.[71]

Device Fingerprinting. In lieu of cookies, a technique called fingerprinting has emerged to maintain access to users who regularly 'clean' their computers. Each device has a unique 'fingerprint' or signature built on a string of data resulting from the operating system, version, and application configuration of that device.[72] More concerning is that when this information is paired with a user's IP address, it often can deliver a level of detail equal to cookies or enable the 'regeneration' of a deleted cookie, thus circumventing sanitation of cookie signatures.[73]

The management of this data is a growing threat to personnel. Aggregation of personal data is generally done by benign actors—marketing firms looking to target consumers—however, more adversarial and malicious actors may utilize it for criminal, military, or intelligence purposes.[74] It should be noted that it is not always clear which entities own, maintain, control or have access to this aggregated data. Due to the data marketplace, the information quickly and frequently changes hands, complicating measures to protect it.[75] Even when steps are taken to properly secure information, nefarious actors utilizing illicit means often compromise data protections, leaving thousands vulnerable. More dangerous to military end-users operating within networks controlled by authoritarian regimes, this data resides on high-risk networks and is readily available to and often controlled by the state.

---

[71] Estrada-Jiménez et al., 38.

[72] Estrada-Jiménez et al., 38.

[73] Mikhail J. Atallah and Nicholas J. Hopper, "Erratum to: Privacy Enhancing Technologies," in *Privacy Enhancing Technologies*, ed. Mikhail J. Atallah and Nicholas J. Hopper, vol. 6205 (Berlin, Heidelberg: Springer Berlin Heidelberg, 2017), 3, http://link.springer.com/10.1007/978-3-642-14527-8_17.

[74] T. X. Hammes, "Technology Converges; Non-State Actors Benefit," *Governance in an Emerging New World*, Winter, no. 319 (February 25, 2019), https://www.hoover.org/research/technology-converges-non-state-actors-benefit; Feldstein, "The Global Expansion of AI Surveillance," 11.

[75] Terry Gross and Dave Davies, "How Tech Companies Track Your Every Move and Put Your Data Up for Sale," *Fresh Air*, July 31, 2019, https://www.npr.org/2019/07/31/746878763/how-tech-companies-track-your-every-move-and-put-your-data-up-for-sale.

E. CONCLUSION

The technological advancements of 5G will bring a monumental shift to the way the world telecommunicates. Fundamental changes to end-user devices, antenna and cell construction, network architecture, and urban and rural infrastructure will be required. However, in many ways, the more interesting question is what fundamental changes will be made to the capabilities enabled by emerging technology and how those resources will be operationalized. Enhanced mobile broadband, massive connectivity, and ultra-reliable low latency characteristics will do more than simply reduce the time it takes to download a file or improve the quality of streaming content. These capabilities, when packaged properly, can enable massive changes to way we go about our day to day lives.

A smart city, one that is connected and synchronized, can streamline traffic and reduce pollution via the IoT. Consumers can interact with their environment via augmented reality, personalized by contextual marketing. Law enforcement and security professionals can monitor, assess, and anticipate criminal and terrorist activity through an integrated CCTV network paired with facial recognition and artificial intelligence. Accomplished at near real-time, each of these applications will depend on the proliferation of reliable and capable 5G networks.

However, as SOF operations remain prolific within contested regions and often where adversarial 5G networks are proliferated, it will be important to understand the vulnerabilities of operating within these “high-risk” networks. Particularly as the distinctions between commercial, dual-use, and purpose-built equipment are reduced, security and signature management risks will challenge operational units to find creative solutions. Armed with a baseline of the emerging technological framework, exploring our adversaries’ strategic intentions—particularly China’s rise as a regional hegemon through the Belt and Road Initiative—as well as the implementation of 5G networks worldwide will inform an assessment of current and future threats to operations.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CHINA AND 5G

> If someone exists, there will be traces, and if there are connections, there will be information.[76]
>
> — China Electronics Technology Corporation Surveillance System Slogan

China's 5G proliferation strategy—a key feature of their Digital Silk Road nested within the Belt and Road Initiative (BRI)—can be viewed through the lens of economic nationalism.[77] From this perspective, recognizing that economic activity is subordinated to the goals and interests of the state fosters a better understanding of their actions and intent.[78] The foremost objective of any economic nationalist regime is state-driven development coupled with approaching international economic relations as a zero-sum game.[79] In today's digital environment, China's modernization of the information and communications technology sectors both at home and abroad creates an environment primed for their rise as an economic powerhouse. As Gilpin argues, when a rising power has a traditional economic nationalist viewpoint, that nation tends to wage economic warfare to satisfy national objectives; China's own admissions and actions demonstrate their intentions to continue their international gains through economic means.[80]

Looking at Japan's rise from the ashes of World War II to economic prominence in the 1980s, we can gather a clear blueprint for economic nationalist activity and growth

---

[76] Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," *The New York Times*, May 22, 2019, sec. World, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

[77] Lars Magnusson, *Mercantilism: The Shaping of an Economic Language* (New York: Routledge, 1994).

[78] Robert Gilpin, "Three Ideologies of Political Economy," in *The Political Economy of International Relations.* (Princeton, N.J.: Princeton University Press, 1987), 31–33.

[79] Theodore H. Moran, "An Economic Agenda for Neorealists," *International Security* 18 (2) (Fall 1993): 211–15.

[80] Robert. Gilpin and Jean Gilpin, *Global Political Economy: Understanding the International Economic Order*, *Global Political Economy: Understanding the International Economic Order* (Princeton: Princeton University Press, 2001); "China: OBOR Will Follow Opportunities, Not Blueprint," *Oxford Analytica Daily Brief Service*, June 21, 2017, http://search.proquest.com/docview/1913904392?rfr_id=info%3Axri%2Fsid%3Aprimo.

which is evident in China today. During the post-war period in Japan, the government recovery strategy favored economic growth and prosperity over personal and individual well-being; large companies were protected and subsidized by the state; and a highly educated workforce was the key to consistent growth and economic success.[81] Following their neighbor's example, the Chinese Communist Party has set out a well-defined strategy involving technological development and investment.[82] Supported through heavily subsidized tech giants such as Huawei and benefiting from a skilled workforce that grew up in the cutthroat tech sectors of Beijing and Shenzhen, the result is a rising power that is utilizing the information and communications technology sector to solidify and catalyze their path to economic hegemony.[83]

To assess the implications more accurately to special operations within a 5G environment, it is important to understand the telecommunications strategy of China, particularly with respect to the manufacturing and end-to-end hardware and software services offered by non-domestic providers. Aligning with their Digital Silk Road strategy, China is now the world's greatest supplier of 5G technology.[84] Using their telecommunications giant Huawei, China has rapidly proliferated their 5G technology—both in infrastructure and software—to vast areas around the world through their Belt and Road Initiative.[85] Established in more nations than any other competitor in the world, Huawei's networks—often packaged as complete end-to-end services to include the hardware and software backbone as well as network controls—make up a significant swath

---

[81] Robert J. Crawford, "Reinterpreting the Japanese Economic Miracle," *Harvard Business Review*, January 1, 1998, https://hbr.org/1998/01/reinterpreting-the-japanese-economic-miracle; Daniel Okimoto, *Between MITI and the Market: Japanese Industrial Policy for High Technology* (Stanford: Stanford University Press, 1990).

[82] "China: OBOR Will Follow Opportunities, Not Blueprint."

[83] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018), 15–16; "China: OBOR Will Follow Opportunities, Not Blueprint."

[84] "My Way or the Huawei: 5G at the Center of US-China Strategic Competition," July 23, 2019, https://www.atlanticcouncil.org/blogs/econographics/my-way-or-the-huawei-5g-at-the-center-of-us-china-strategic-competition/.

[85] Mishra, "Here Are the Countries That Allowed Huawei to Build 5G."

of the BRI's Digital Silk Road.[86] Geographically, the BRI overlaps with U.S. military operations in many regions. As a result, the United States and its allies need to accept the fact that many foreign telecommunication networks around the world must be regarded as "high-risk."[87]

A. THE STRATEGIC NATURE OF CHINA'S 5G EFFORTS—A DIGITAL SILK ROAD

Guidance from the leadership of the Chinese Communist Party (CCP) has driven China to aggressively transform its economic foundation from industry and manufacturing to information and digital technology.[88] In doing so, the government began heavily subsidizing Chinese technology firms during the 1990s and early 2000s, attempting to rapidly become the next world leader in digital and telecommunications technology.[89]

China's BRI strategy seeks to create a near continuous sphere of economic influence and support across the globe, cementing their rise as the next global superpower; in support of this long term initiative, China's largest information, communication, and technology (ICT) companies are currently operating in nations along the BRI.[90] Utilizing these companies, China is not only striving to expand their economic base by opening up digital marketplaces, but also seeking to own the information environment as well.

Kai-Fu Lee warns that China is positioning itself in the modern digital age akin to Saudi Arabia's position in the oil industry.[91] In an industrial economy where oil was the foremost sought-after natural resource, nation-states lashed their economic futures and national defenses to oil reserves. In the digital information age, however, the internet-based

---

[86] Mishra.

[87] Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 29.

[88] Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, 2–4.

[89] Lee, 2–4, 84, 98–100.

[90] "China: Digital Silk Road Will Boost China's ICT Sector," *Oxford Analytica Daily Brief Service*, January 22, 2018, http://search.proquest.com/docview/1989534760/.

[91] Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, 50, 55–56.

and inter-connected mobile economy will likely enable data to replace oil as the world's most important economic resource.[92]

China—the most populous nation on earth—maintains over 100 cities with populations over a million people and is sitting on the largest potential resource of data of any country.[93] As a result of vast data resources and a "government-accelerated," tech-driven economy, Chinese companies such as Alibaba, Tencent, Baidu, and Huawei are less encumbered by market restrictions than their Western counterparts and have a marked advantage in developing software, tools, and technologies.[94] Their substantial resources allied with the dizzying pace of their market economy allow Chinese firms to implement, test, and evaluate myriad technologies at rates faster than any other nation in the world.[95] During the rapid race to 5G, China has mirrored this approach in their BRI strategic trajectory, combining their immense domestic data resources and rapid technological fielding with international influence.[96] As history has shown in previous rollouts of 3G and 4G/LTE—Europe and the United States enjoyed the first-mover advantage during these technological advancements, respectively—to the winner goes the economic spoils.[97] China is currently winning the 5G race, with Huawei as their foremost thoroughbred.

B. HUAWEI—CHINA'S LEADER IN 5G

Huawei, China's premier ICT company, is the largest telecommunications manufacturer and provider in the world.[98] Headquartered in Shenzhen, China, it has established operations in more than 170 countries and employs over 188,000 personnel.

---

92 Lee, 50.

93 Lee, 99.

94 Lee, 40, 99.

95 Lee, 26–28, 44, 49–50.

96 "China: Digital Silk Road Will Boost China's ICT Sector."

97 Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*.

98 Kyle Almond, "A Rare Look Inside Huawei, China's Tech Giant," *CNN*, May 2019, sec. Business, https://www.cnn.com/interactive/2019/05/business/huawei-cnnphotos/index.html.

Huawei's strength comes from their size and their ability to offer end-to-end telecommunications services to most any region throughout the world.[99]

Much of Huawei's current might is the result of the CCP's support; since 1987, following their rise from a telephone switch company to a global telecommunications powerhouse, the firm has received more than $75 billion dollars in subsidies from the CCP.[100] These subsidies have manifested in deals on land to build infrastructure, tax breaks nearing $25 billion dollars, and significant financial grants. Between 2013 and 2018, Chinese government grants to Huawei were 17 times larger than Finnish grants to Nokia while Swedish competitor, Ericsson, did not receive any government grants.[101]

Given the level of governmental financial support offered to Huawei, it is hard to argue that Huawei does not have significant ties to the government. These connections to the CCP go beyond simply boosting economic strength, however; Chinese law and policy necessitates the cooperation of Chinese telecommunication firms—state-sponsored or not—to participate in intelligence gathering activities.[102] The combination of government patronage with legal obligations to participate in domestic surveillance and the theft of international intellectual property has led to the U.S. government's sweeping ban against Huawei, as well as significant political pressure abroad to institute similar restrictions.[103]

Despite the U.S. government's attempts to quell Huawei's influence around the world, the telecommunications giant remains the chief competitor of other powerhouses such as Samsung, Ericsson, and Nokia; particularly as Huawei expands 5G technology throughout the developing world and along the digital silk road, Huawei's key

---

99 "Public Policy Position: 5G Spectrum."

100 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, December 25, 2019, sec. Tech, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

101 Yap.

102 Tom Wheeler and Robert D. Williams, "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G," in *Huawei, 5G and National Security: A Lawfare Compilation* (Washington, DC: Lawfare Institute, 2019), Chapter 1, pg 2, www.lawfareblog.com.

103 Wheeler and Williams, "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G."

characteristics keep them as a force to be reckoned with.[104] One of the main strengths Huawei enjoys is the experience, expertise and capabilities of their people. Kai-Fu Lee notes that those working at Huawei are often tech-savvy entrepreneurs who grew up in the cutthroat Chinese technology market of the 2000s and 2010s.[105] He argues that, as a result of the Chinese hyper-competitive technology sector, China's workforce is forced to adapt, come up with innovative ideas, and wage economic war on each other's companies. As a result, Huawei's personnel understand the merciless business better than those brought up protected by Western policies enjoyed in Silicon Valley. Bolstered by the most capable engineers, innovators and technical experts in the field, Huawei's aggressive navigation of this emerging field allowed them to enjoy a first-mover advantage in many regions years before many other competitors began to even familiarize themselves with 5G.[106]

C. CHINESE 5G PROLIFERATION

By far, one of their strongest attributes is Huawei's ability to offer end-to-end telecommunications services that are inexpensive. With substantial government financial support, Huawei is able to offer products and services 30% cheaper than their competitors and often without political and diplomatic strings attached.[107] When leveraged in developing areas, often along the BRI, Huawei's model may be difficult or near impossible for these actors to turn down as they strive to keep up with modern development and globalization. As previously discussed, many of these nations are in regions of interest to special operations forces. And despite the ability of U.S. military operations to provide stand-alone communications, it is not uncommon for these forces to rely, at least partially, upon indigenous communications networks.

---

104 John T. Watts, "A Framework for an Open, Trusted, and Resilient 5G Global Telecommunications Network," *Atlantic Council*, March 2020, 6, https://www.atlanticcouncil.org/wp-content/uploads/2020/03/Framework-for-a-5G-Network.pdf.

105 Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*.

106 Almond, "A Rare Look Inside Huawei, China's Tech Giant"; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 6.

107 Yap, "State Support Helped Fuel Huawei's Global Rise."

Already operating in 170 countries, Huawei's products and services are highly rated and sought after in many regions.[108] Combined with a price point well below what many competitors can offer, it is no surprise Huawei is winning the race to 5G. Showing a distinct capability to market in, deploy to, and invest in foreign markets like no other telecommunications company, they continue to aggressively test, evaluate and market their 5G telecommunications systems around the world and have won a multitude of long term contracts.[109]

1. Huawei's Worldwide Investments

In the face of the federal U.S. ban on utilizing Huawei equipment within domestic and government networks, as well as diplomatic pressure on allies to institute similar polices, the Chinese firm is still outperforming international competitors. Even the United States' closest ally and member of the Five-Eyes intelligence sharing agreement, the United Kingdom, has been reluctant to ban Huawei from its telecommunications system.[110] By early 2020, Huawei has secured over fifty 5G contracts in multiple countries throughout Asia and the Middle East as well as emerging contracts in Europe and South America.[111]

As shown in Figure 6, existing Huawei infrastructure in large swaths of Africa, the Middle East and South America will likely allow further Chinese investment; Huawei's attractive price points combined with infrastructure investments and a high level of political commitment from Beijing are critical factors allowing for Chinese technological proliferation.[112] Additionally, Huawei's accelerating expansion throughout Europe is also

---

[108] Almond, "A Rare Look Inside Huawei, China's Tech Giant"; Daniel Araya, "Huawei's 5G Dominance in the Post-American World," *Forbes*, April 5, 2019, https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/; Antonio Villas-Boas and Lisa Eadicicco, "Why Huawei Smartphones Are Popular All Over the World, Except the US," *Business Insider*, May 20, 2019, https://www.businessinsider.com/huawei-smartphones-are-popular-all-over-world-not-united-states-2018-12.

[109] Rita Liao, "Huawei Says Two-Thirds of 5G Networks Outside China Now Use Its Gear," *TechCrunch* (blog), June 25, 2019, http://social.techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

[110] BBC Click, "Inside Huawei and 5G," https://www.youtube.com/watch?v=_8HqbPBRiS4.

[111] Liao, "Huawei Says Two-Thirds of 5G Networks Outside China Now Use Its Gear."

[112] "China: Digital Silk Road Will Boost China's ICT Sector."

a clear indicator of the tech giant's influence in regions not typically vulnerable to economic manipulation.[113] Gaining a significant foothold in Europe, Huawei announced plans in 2019 to build two research centers in Switzerland, as well as pledging $3.1 billion dollars to Italy's network infrastructure.[114] Worldwide, Huawei has recently claimed that nearly two-thirds of 5G networks outside of China utilize, at least partially, Huawei equipment.[115]

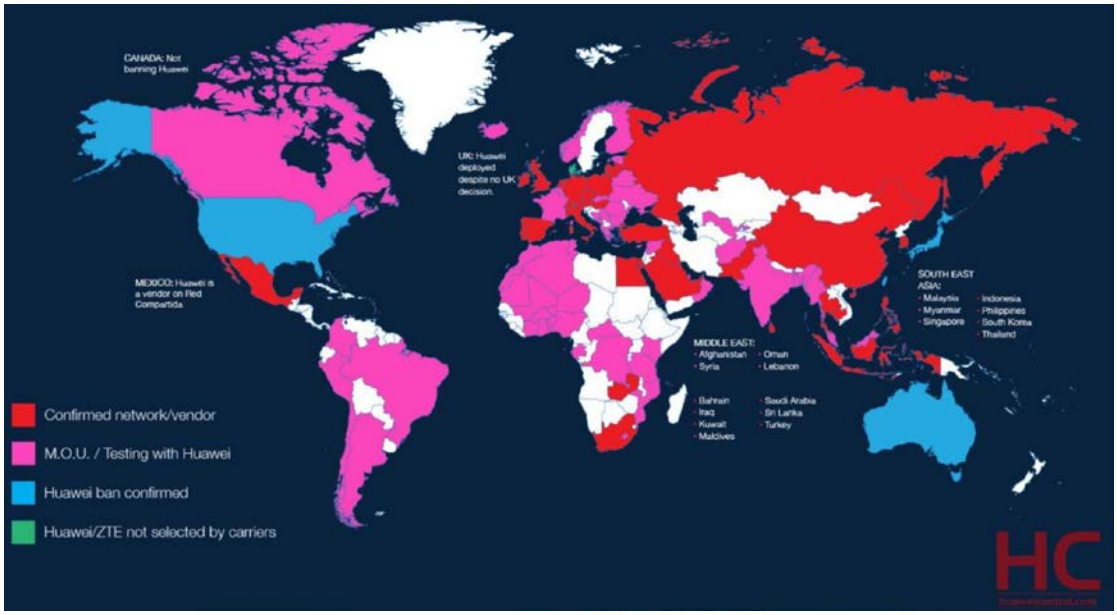


Figure 6. Huawei's Worldwide 5G Footprint[116]

As previously discussed, this level of Chinese investment in international infrastructure is not unprecedented. Along the BRI, China's digital silk road has expanded coverage to traditionally underserved populations and has upgraded the infrastructure

---

113 Emily Feng and Amy Cheng, "China's Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts to Ban It," *National Public Radio*, October 24, 2019, sec. World, https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it.

114 Feng and Cheng.

115 Liao, "Huawei Says Two-Thirds of 5G Networks Outside China Now Use Its Gear."

116 Source: Mishra, "Here Are the Countries That Allowed Huawei to Build 5G."

within existing telecommunication architectures at extremely competitive prices.[117] Often, the end-to-end services are offered with perks that seem too good to be true—particularly to authoritarian states keen on taking advantage of so-called surveillance packages—yet, the unforeseen costs in terms of influence, control, security, debt traps, and limited domestic work opportunities may outweigh any benefit gained by partnering with Huawei.[118] An example of such a case is China's infrastructure investments within Cambodia—the Unites States once enjoyed much stronger ties to the Association of Southeast Asian Nations (ASEAN) member-state, however, Cambodia recently suspended joint military operations in favor of its relationship to China.[119] Regionally strategic due to its proximity to other United States allies and the South China Sea, it may prove beneficial to look at this specific example in order to analyze the risk associated with such an environment and the impact of partnership with China and Huawei.

2. Cambodia—A Chinese 5G Vignette

Huawei's investment in Cambodia provides a keen example of effective proliferation of Chinese technology, increasing control, influence, and information awareness for the CCP. Despite the United States' efforts to maintain political influence in Cambodia—its proximity to mainland China and the South China Sea adds significantly to

---

117 "China: Digital Silk Road Will Boost China's ICT Sector"; Shaun Turton and Tomoya Onishi, "Cambodia 5G Set to Leapfrog ASEAN Rivals with Huawei and ZTE," *Nikkei Asian Review*, September 5, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Cambodia-5G-set-to-leapfrog-ASEAN-rivals-with-Huawei-and-ZTE; Milcah Lukhanyu, "Huawei to Build Sh17.5b Konza Data Centre and Smart Cities Project," *TechMoran*, April 27, 2019, https://techmoran.com/2019/04/27/huawei-bags-chinese-govt-deal-to-build-sh17-5b-konza-data-centre-and-smart-cities-project/; Mishra, "Here Are the Countries That Allowed Huawei to Build 5G."

118 Watts, "A Framework for an Open, Trusted, and Resilient 5G Global Telecommunications Network," 6; Ryan Maness, "Chinese Cyber Behavior: Manipulation and Espionage," lecture (Monterey, CA: Naval Postgraduate School, November 7, 2019); Prak Chan Thul, "Cambodia PM Dismisses Fears of Chinese Debt Trap," *Reuters*, May 30, 2019, sec. World News, https://www.reuters.com/article/us-cambodia-china-idUSKCN1T00U8; "Mike Pompeo Urges Tories to Ask: 'What Would Thatcher Do?,'" *The Guardian*, May 8, 2019, sec. Technology, https://www.theguardian.com/technology/2019/may/08/mike-pompeo-invokes-thatcher-push-harder-line-china-huawei.

119 Prak Chan Thul, "Cambodia Kicks Off Drills with 'Great Friend' China as U.S. Ties Sour," *Reuters*, March 17, 2018, sec. World News, https://www.reuters.com/article/us-cambodia-china-military-idUSKCN1GT05F.

its strategic value—ties between Phnom Penh and Beijing have grown over recent years.[120] Cambodia's market conditions are representative of how low-cost end-to-end telecommunications services paired with political and economic corruption produce an environment ripe for Huawei's manipulation and proliferation.[121]

China is now Cambodia's largest foreign investor; in 2017 and 2018, China's investments in Cambodia accounted for nearly 25% of the $2.9 billion of annual foreign direct investments, and exceeded the combined investments of the 10 member states of the Association of Southeast Asian Nations (ASEAN).[122] High investment in the country's telecommunication network—often backed by pro-Chinese policies—represents China's particular interest in this industry. More recently, in April of 2019, Telecom Cambodia—a state-run telecommunications company—signed an agreement with Huawei to roll out 5G nationwide in 2020.[123]

Denying significant political and diplomatic influences within the country, Cambodian telecommunications executives frame the decision to partner with and utilize Huawei's end-to-end services as a decision driven purely by economic competition.[124] In order to manage their company's success and their ability to compete with others, executives must look at technological compatibility, security and cost while overlooking the foreign influence that is often married to the deal. More often than not, in markets like Cambodia, executives prioritize cost over other factors in order to roll out technology, gain the first mover advantage, and defeat industry peers by offering new services to the local

---

120 Phillip Orchard, "China's Plan to Win Over Cambodia," *Real Clear*, August 1, 2019, sec. World, https://www.realclearworld.com/articles/2019/08/01/chinas_plan_to_win_over_cambodia_113068.html.

121 Andrew Nachemson and Kong Meta, "Cambodia's Digital Surveillance Is Silencing Government Critics," *Post Magazine*, October 19, 2019, https://www.scmp.com/magazines/post-magazine/long-reads/article/3033508/cambodias-digital-surveillance-serves-silence.

122 Wee Kee Hwee and Amelia Santos Paulino, "ASEAN Investment Report 2019" (Jakarta, Indonesia: ASEAN Secretariat and United Nations Conference on Trade and Development, 2019), 9, https://unctad.org/en/PublicationsLibrary/unctad_asean_air2019d1.pdf.

123 Turton and Onishi, "Cambodia 5G Set to Leapfrog ASEAN Rivals with Huawei and ZTE."

124 Turton and Onishi.

population.[125] As a result, Huawei's appeal once again is the low-cost solution, thereby more frequently winning crucial telecommunications contracts to build the emerging 5G networks.

Proliferation within Cambodia will be phased incrementally, initially focused on urban centers, targeting greatest population density and cost reduction. Cellcard, one of Cambodia's largest telecommunications companies, plans to install five hundred small cell 5G base stations in three of the country's largest cities—Phnom Penh, Siem Reap and Sihanoukville—during its first phase of the rollout.[126] Though these small cells are provided by ZTE—another state-controlled Chinese tech company that has been banned by the United States—Cellcard's strategy also includes a great deal of support from Huawei equipment and expertise.[127] This common pattern of early installation in densely populated urban areas will be a standard practice for worldwide 5G implementation. The cost of integrating adequate 5G architecture into legacy network infrastructure will initially reduce the sprawl of 5G technology into rural areas. The distinction between urban and rural networks—at least for the near term—may have significant impacts on SOF operations; since the telecommunication architectures will not be homogenous throughout a particular area of operations, it will be critical for mission analysis to understand the coverage, overlap, and gaps of each network type.

Although the adoption of Huawei or ZTE based networks may draw short term economic gain for Cambodia and the large business entities within, there are significant costs and negative repercussions in other arenas. First and foremost, the control and influence that the Chinese Communist Party maintains of their domestic corporations is great.[128] With Chinese 5G networks in place, China will own, perhaps de facto, the telecommunications infrastructure and, in turn, own the information environment. In an era

---

[125] Turton and Onishi.

[126] Turton and Onishi.

[127] Turton and Onishi.

[128] Feng and Cheng, "China's Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts to Ban It."

when information warfare rivals conventional means of power, this is of significant concern not only to the people of Cambodia but also to the United States and other Western countries.[129] The addition of Chinese 5G networks in Cambodia also creates even greater economic dependence on the Eastern hegemon. When the reliance on China for the technology and expertise is combined with an alignment of the authoritarian Cambodian government with Beijing, there is significant cause for concern in the area of state-run technical surveillance as well.[130] The costs of adopting Chinese 5G networks far outweigh their short-term benefits—the total impacts of which may not be seen for years to come.

D. HIGH-RISK NETWORKS ARE THE NORM

According to a Carnegie Endowment assessment, Huawei maintains a significant presence via infrastructure and artificial intelligence-based surveillance in many developing nations.[131] Many of these regions overlap with areas the United States and its allies actively conduct activities to counter violent extremist organizations—namely the Middle East and Africa—as well as areas where great power competition has begun to reemerge—Eastern Europe and Asia. As we look at current proliferation efforts and trends, it is likely that Huawei—and more pointedly China—will own an even greater share of the global telecommunication networks, particularly in the 5G domain. Given the fact that an adversary and technological peer owns this infrastructure, it is imperative that we recognize the networks our forces are operating within are likely high-risk networks; it should be assumed that communications are monitored, activities surveilled, and physical and digital patterns of activity are acutely studied. Furthermore, it should be assumed that the more we rely on and operate within high-risk networks, the likelihood of cyberattack and cyber vulnerability increases.

Expecting the convergence of 5G technology and artificial intelligence, special operations forces should anticipate vulnerabilities to manifest in ubiquitous technical

---

129 Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder* (New York: William Morrow, 2019), 8–9.

130 "Cambodia Profile," *BBC News*, July 9, 2014, sec. Asia, https://www.bbc.com/news/world-asia-pacific-13006542.

131 Feldstein, "The Global Expansion of AI Surveillance," 25–28.

surveillance and weaponized advertising technology. Posing significant challenges to the conduct of special operations, these threats have the potential to remove the element of surprise and the plausible deniability so vital to maintaining operational security, force protection, and reducing overall risk to mission.

1. Ubiquitous and State-Run Technical Surveillance Threat

The adoption and implementation of 5G networks, characterized by an increased ability to network devices, expanded bandwidth, and reduced latency, will hyper-enable technical surveillance networks. The previously limited IoT will now be able to integrate more devices (cameras, microphones, biometric monitors, smart TVs, autonomous vehicles, etc.), collect and transmit information from those devices faster, and process the data using deep learning and artificial intelligence, creating near real-time situational awareness for an adversary.

Not only does Huawei supply 5G equipment, but they and other Chinese firms, such as ZTE and Hikvision, also supply the AI-supported surveillance systems that will run on these networks.[132] Shown in Figure 7, Huawei, by far, is the leading global supplier of advanced technical surveillance technology.[133]

[132] Feldstein, "The Global Expansion of AI Surveillance."

[133] Feldstein.

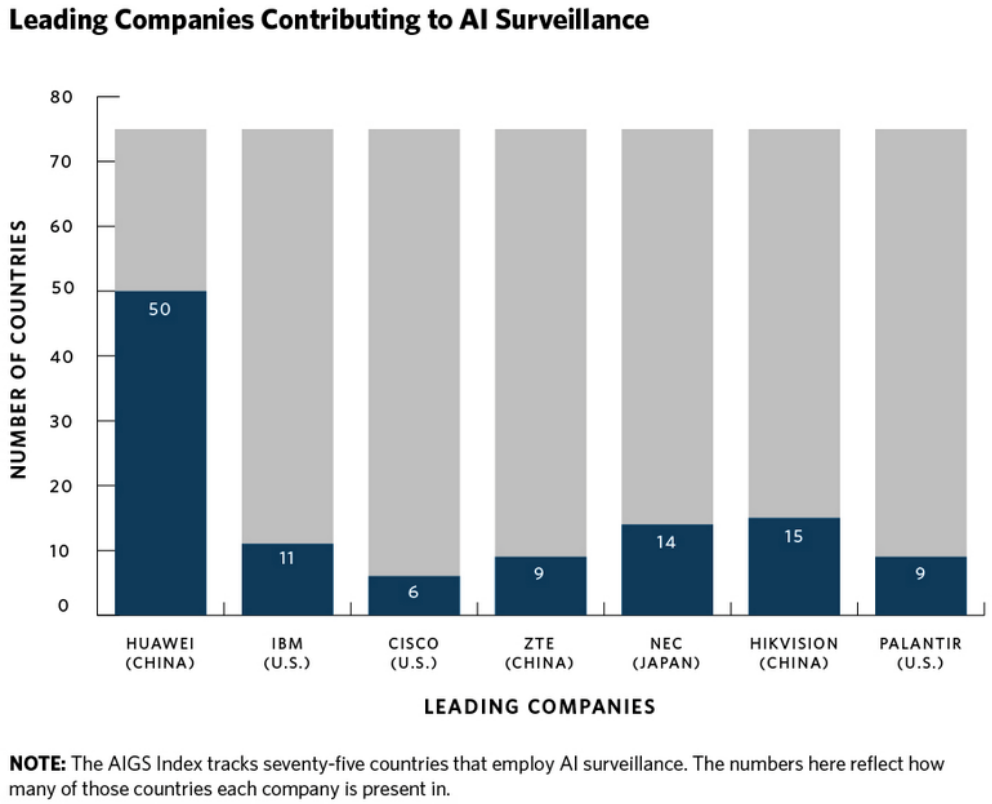


Figure 7. Leading Companies Contributing to AI Surveillance[134]

China offers these surveillance systems as a complete package; from installation of the cameras all the way to building a surveillance command center, China's "surveillance packages" are attractive to authoritarian governments looking for more robust social control as well as more liberal nations looking for law-enforcement and national security options. Table 1 offers insight into not only where AI-enabled surveillance has been proliferated, but also the nature in which the AI has been utilized.

[134] Source: Feldstein, 9.

Table 1. Focused Selection from the AI Global Surveillance Index[135]

Country	Regime Type	"Freedom on the Net 2018" Status	Military Spending Ranking (2018)	Five Eye?	BRI Country?	Smart/Safe City?	Facial Recognition?	Smart Policing ?	Chinese Tech?	U.S. Tech?	Key Companies
Australia	LD	FREE	13	X		X	X	X	X	X	CrowdOptic, Hikvision, Huawei, Infinova, NEC, Palantir
Canada	LD	FREE	14	X			X	X		X	Hikvision, Huawei
China	CA	NOT FREE	2			X	X	X	X	X	Mult; Axis, Bosch, IBM, Microsoft, Seagate, Qualcomm
Germany	LD	FREE	8			X	X	X	X	X	Cisco, Huawei, Palantir
Hong Kong	ED						X		X		Bosch, Huawei
India	ED	PARTLY FREE	4			X	X	X	X	X	ADRIN, Hikvision, IBM, Infinova, Microsoft, NEC
Iran	EA	NOT FREE	18		X		X	X	X		Hikvision
Iran	EA		32		X	X	X		X		Huawei
Italy	LD	FREE	11		X	X			X		Huawei
Japan	LD	FREE	9			X	X	X	X		Hikvision, NEC
Kazakhstan	EA	NOT FREE	64		X	X	X	X	X		Analytical Business Solutions, Huawei, Speech Technology Center
Kenya	EA	PARTLY FREE	69		X	X	X	X	X		Huawei, NEC, Safaricom
Kyrgyzstan	EA	PARTLY FREE	118		X	X	X	X	X		Huawei
Malaysia	ED	PARTLY FREE	49		X	X	X	X	X		Huawei, NEC, Yitu
New Zealand	LD		56	X	X		X	X		X	Palantir
Pakistan	EA	NOT FREE	20		X	X	X	X	X		Huawei
Philippines	ED	PARTLY FREE	46		X	X	X	X	X	X	Boeing, CITCC, IBM, Huawei
Russia	EA	NOT FREE	6		X	X	X	X	X	X	Analytical Business Solutions, Cisco, Huawei, NtechLab, Speech Technology Center
Saudi Arabia	CA	NOT FREE	3		X	X	X	X	X	X	Briefcam, Gatekeeper, Hikvision, Huawei, Hugslock, IBM, NEC
Singapore	ED	PARTLY FREE	22		X	X	X	X	X	X	Accenture, AGT, Airbus, Dassault, Huawei, NEC, Tascent, Yitu
South Korea	LD	FREE	10		X	X	X	X		X	Axis, IBM, Korea Telecom, LG Uplus, SK Telecom
Ukraine	ED	PARTLY FREE	39		X	X	X		X	X	Hikvision, Huawei, Microsoft
United Kingdom	LD	FREE	7	X		X	X	X	X	X	Hikvision, NEC, Palantir
United States	LD	FREE	1	X		X	X	X	X	X	Mult; Amazon, Hikvision, IBM, Infinova, Palantir, PredPol, Pelco, Avigilon

One of the more concerning capabilities that China exports, specifically through Huawei, is facial recognition. As part of its "safe city" platform exported to foreign markets, Huawei offers advanced facial recognition software and hardware; these packages generally include robust video surveillance as well as AI software support. Huawei built their first "safe city" in Nairobi, installing more than "1,800 cameras and 200 traffic

135 Adapted from Feldstein, 25–28.

surveillance systems."[136] Likewise, in the French cities of Marseille and Valenciennes, ZTE and Huawei have partnered with local officials to implement "safe city" technology paired with big data AI networks; Valenciennes was *gifted* a full surveillance package that included high definition CCTV as well as an AI-driven command center to identify suspicious persons, crowds, or actions.[137]

However, facial recognition is not the only concern with respect to newly integrated devices. As more devices join the network, the pairing of 5G and AI will be even stronger. AI depends upon more and more data points to create a more accurate, timely intelligence picture. Armed with that knowledge, government agencies, law enforcement, and even bad actors can target adversaries. The willingness and intent to engage in such activities has already been demonstrated around the world; in Uganda and Zambia, Huawei technology, as well as their employees, was utilized to spy on political opponents, "intercepting their encrypted communications and social media, and using cell data to track their whereabouts."[138] Achieved by utilizing the basic data available from legacy networks, these capabilities will continue to mature as 5G and AI are adopted into the mainstream.

2. Advertising Technology-Based Threat

The pairing of 5G and AI does not simply improve technical surveillance capabilities; as discussed in Chapter II, the power of advertising technology and its potential to become weaponized continues to grow. Particularly as social patterns of behavior continue to normalize the surrender of personal privacy, advertising technology remains a powerful tool for marketing, social control, and potentially in the future, military

136 "Video Surveillance as the Foundation of 'Safe City' in Kenya," 2019, https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya.

137 Feldstein, "The Global Expansion of AI Surveillance," 10–11.

138 Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *The Wall Street Journal*, August 15, 2019, sec. Tech, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017; Feldstein, "The Global Expansion of AI Surveillance," 14.

action.[139] The legacy 4G networks have already enabled markets around the world to capitalize on the marketing potential of contextualized, real-time or just-in-time advertising; however, we are just beginning to see the impacts these technology tools may have on social control and policing actions.[140] The emergence of 5G technology paired with more advanced AI will accelerate their development and bolster the utility of these capabilities.

China's synthesis of online-to-offline applications (e.g., "real-world internet services" such as ride-sharing, meal delivery, or peer-to-peer financial transfers), AI analysis, and the proliferation of more integrated surveillance packages paired with data derived from advertising technology has become the standard-bearer for social and political control.[141] Forms of data commonly used in advertising technology, as well as the advertising technology platforms themselves, are easily adapted to surveille individuals and predict their future behaviors. Throughout China today, these practices are already being utilized by intelligence collectors to develop profiles, track individuals, and anticipate decision-making, movement, and other actions.

In regions all across China, "algorithmic governance" is being developed, implemented, and refined.[142] Police in Kashgar enter suspicious behavior into mobile app databases; extended travel, refueling someone else's vehicle, using an *unusual* amount of

---

[139] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, July 8, 2018, sec. Business, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[140] David Kirkpatrick, "Why Just-In-Time Trumps Real-Time for Marketing Efficiency," *Marketing Dive*, October 17, 2016, https://www.marketingdive.com/news/why-just-in-time-trumps-real-time-for-marketing-efficiency/422353/; Zuboff, "'Surveillance Capitalism' Has Gone Rogue. We Must Curb Its Excesses."; Buckley and Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities"; Paul Mozur and Aaron Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers," *The New York Times*, December 17, 2019, sec. Technology, https://www.nytimes.com/2019/12/17/technology/china-surveillance.html; Charlie Campbell, "The Entire System Is Designed to Suppress Us: What the Chinese Surveillance State Means for the Rest of the World," *Time*, November 21, 2019, https://time.com/5735411/china-surveillance-privacy-issues/.

[141] Lee, *AI Superpowers: China, Silicon Valley, and the New World Order*, 68; Buckley and Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities"; Campbell, "The Entire System Is Designed to Suppress Us"; Mozur, "Inside China's Dystopian Dreams"; Mozur and Krolik, "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers."

[142] Mozur, "Inside China's Dystopian Dreams."

electricity, or discontinuing use of a smartphone may all qualify as suspicious behavior.[143] Police are utilizing glasses enabled with facial recognition while the travel patterns, internet use, and social engagements of citizens are monitored.[144] The nation's two hundred million surveillance cameras—nearly four times the number of cameras in the United States—track faces, clothing, gait, and behavior.[145] Analysis of this information is largely done by humans and occasionally augmented by automation; however, the Chinese police plan to spend nearly $30 billion to empower AI and "techno-enabled snooping" techniques.[146]

China's surveillance economy has grown beyond marketing and into social control; the commitment to monitoring their population has fueled immense research and development initiatives.[147] State-media propaganda recently released a film touting the benefits of surveillance and the potential of predictive policing.[148] China's surveillance capabilities do not yet fulfill the dystopian vision of the film; however, as AI technology continues to advance and the volumes of data required to refine algorithms is delivered by a more connected 5G world, predictive policing may not be too far off. One main worry of political activists in the region is that once the capabilities of AI are fully realized, advanced "forensic safeguards may not be enough" to protect against government overreach and abuse.[149]

E. CONCLUSION

As advertising technology-based threats are refined and proliferated around the world, it is likely that social control will not be its only use; the veil of secrecy once enjoyed

---

143 Buckley and Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities"; Campbell, "The Entire System Is Designed to Suppress Us."

144 Mozur, "Inside China's Dystopian Dreams"; Campbell, "The Entire System Is Designed to Suppress Us."

145 Mozur, "Inside China's Dystopian Dreams."

146 Mozur.

147 Mozur.

148 Mozur.

149 Campbell, "The Entire System Is Designed to Suppress Us."

by our special operations forces is at risk. High-risk, adversarial 5G networks are proliferating around the world and into many of the regions in which special operations missions are focused. When an adversary owns the telecommunications infrastructure, these operations are at risk of highly sophisticated surveillance utilizing artificial intelligence to analyze the abundance of data available (both anonymized and non-anonymized). It is imperative we understand the implications of working in this realm and empower a shift in our methods, tradecraft, and the mindset of our men and women before stepping foot onto the battlefield.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SIGNATURE MANAGEMENT IMPLICATIONS IN 5G

> For the first time in human history, it is near impossible to be unobserved.[150]
>
> —GEN Mark A. Milley

Traditionally, successful special operations missions have relied on security, or secrecy, as well as their ability to capitalize on the element of surprise.[151] These principles, among others, give special operations teams key advantages over an adversary that may otherwise enjoy relative superiority. A team that can effectively control the flow of information relative to their mission objectives, actions, and capabilities has a greater chance of achieving security and surprise. The adversary's knowledge of this critical information is only gained by what they can observe—the physical and digital signature of an operation—and, therefore, the protection of this data is commonly referred to as signature management. However, as we have shown, the pervasiveness of surveillance and advertising technologies enhanced by 5G networks and artificial intelligence will challenge the ability to manage information to the same degree as special operations teams of the past. A brief exploration of signature, signature management, and deception (a tool that is sometimes employed to manage information) will help to clarify the implications of this emerging technological reality.

A. SIGNATURE MANAGEMENT AND DECEPTION

Drawing upon Dr. Kent Andersson and others, this thesis defines a signature as a *set of unique and identifying characteristics, often in specific combination or aggregation, allowing for identification of a specific object, action, or phenomenon within an*

---

[150] P. W. Singer and Emerson T. Brooking, "Social Media Is Revolutionizing Warfare," *The Atlantic*, October 2, 2018, sec. Global, https://www.theatlantic.com/international/archive/2018/10/likewar-internet-new-intelligence-age-flynn/571903/.

[151] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice* (Novato, CA: Presidio, 1995), 10–15.

environment.[152] In his thesis on signature management, Andersson highlights that signatures are observable characteristics of an entity by one or more sensors; signatures may present themselves in several forms, including electromagnetic waveforms, digital behavior, or visible characteristics.[153] Signatures become actionable by an adversary when the information collected is paired with the context of the observation; risk to force and risk to mission are increased dramatically if this signature is not effectively managed, ultimately projecting unwanted information about the timing, nature, or location of an operation.

Signature management—active and passive alterations to an entity's contrast to its ambient environment—therefore, is a tool for military strategists, operational and tactical planners as well as the operators to maintain operational security (OPSEC) and retain the critical element of surprise.[154] Altering a signature, ultimately, is a form of deception. J. Bowyer Bell concludes that "deception is the conscious, planned intrusion of an illusion seeking to alter a target's perception of reality, replacing objective reality with perceived reality."[155] By this definition, we see that deception is a deliberate action or set of actions specifically intended to change the mindset and, in turn, the decisions of those we intend to deceive.

Effective deception relies on and takes advantage of perceptual and cognitive biases; humans tend to perceive what is expected, and their own expectations tend to

---

[152] Kent Andersson, "On the Military Utility of Spectral Design in Signature Management: A Systems Approach" (PhD diss., Helsinki, National Defence University, 2018), ix, https://www.doria.fi/bitstream/handle/10024/152611/Andersson_thesis_full%20%28web%29.pdf?sequence=1&isAllowed=y; J. Bowyer Bell, "Toward a Theory of Deception," *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (April 2003): 244–79, https://doi.org/10.1080/08850600390198742; Barton Whaley, "Chapter 44: Lessons from Behind Other Hills: Planning Deceptions in 145 Different Disciplines," in *The Art and Science of Military Deception* (Boston: Artech House, 2007).

[153] Andersson, "On the Military Utility of Spectral Design in Signature Management: A Systems Approach," 1.

[154] Andersson, x.

[155] Bell, "Toward a Theory of Deception," 244.

condition what they perceive.[156] *Joint Publication 3-13.4, Military Deception* further supports deception's ability "to deliberately mislead [adversarial]…decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[157] If possible, the steadfast tool of deception would be of great assistance to operators and missions in future 5G environments. Traditionally, deception is relatively cheap in terms of manpower and resources to employ, and, when done effectively, can alter or confuse the situational awareness that an adversary may have gained.

In defining his theory of deception, Bell notes two key modes of deception that obstruct the target's ability to observe or to orient during the decision cycle: dissimulation and simulation.[158] Bell explains that dissimulation is the act of hiding a characteristic or signature to mask the identity, location, intention, or action of an entity; this effectively inhibits the ability to observe. For example, a criminal enterprise may operate a commercial shipping vessel without utilizing the Automatic Identification System (AIS) transponder, effectively hiding its location due to the lack of radar and geolocation information.

On the other hand, Bell expands, simulation is the act of showing a characteristic or signature to obfuscate the identity, location, intention, or action of an entity. An example of this would be a criminal element that operates a commercial shipping vessel while utilizing the AIS transponder signal of a different ship, effectively obfuscating its actions due to the altered signature; this effectively inhibits the ability to orient. It is important to note that dissimulation and simulation are always done in tandem; in other words, something will always be shown—even if it is a blank radar screen—while the true signature will be hidden.

---

156 Hy Rothstein and Barton Whaley, *The Art and Science of Military Deception* (Boston: Artech House, 2013), 107–10.

157 Joint Chiefs of Staff, *Joint Publication 3-13.4, Military Deception* (Joint Chiefs of Staff, 2012), I–1, https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.

158 Whaley, "Chapter 44: Lessons from Behind Other Hills: Planning Deceptions in 145 Different Disciplines," 405.

To further highlight how a small special operations team projects a signature and the growing likelihood of surveillance of operations in a 5G environment, it may prove valuable to offer a short vignette. The vignette below will seek to paint a picture of the threats a special operations team may face while operating in high-risk 5G network environment.

OPERATION GREEN WALL

In this operation, a small team of special operators has been assigned to support missions within INDOPACOM in the small country of Hanu. Their objectives are: insert into an area, link up with indigenous forces, and establish relations for future irregular and asymmetric warfare training, and conduct reconnaissance on potential beach landing sites, helicopter landing zones, safe houses and other areas of interest to facilitate a potential insertion of a larger force.

Though Hanu is of significant strategic importance to the United States and its allies, the Hanuan government also maintains close ties to China. Within the regional hegemon's sphere of influence, like many other countries in this area, the Hanuan government has welcomed state-controlled Huawei to establish the full suite of 5G telecommunications network and associated infrastructure throughout the country. To sweeten the deal, Huawei has thrown in a robust, centrally controlled surveillance system.

The team, like many American special operations units, is racially homogenous, distinctively Western, and projects a physical signature that does not normally blend into the local communities of Hanu. They have received limited training in physical countersurveillance, have taken cybersecurity courses to manage their personal devices, and are rated as 'fit to deploy' by their home unit. Each member deployed with his personal computers and cell phones, though each will also utilize on local cell phones provided by the Special Operations Forces Liaison Element and Defense

Attaché at the United States Embassy for basic intra-team communication. The team's 18E, or Communications Sergeant, has stressed the importance of not transmitting sensitive data or information via the local cell phones as the networks are likely monitored and assessed as high-risk. If needed, the team has access to secure communications at the U.S. Embassy.

Upon arrival via commercial air into the main port of entry, the team makes their way to customs. Each team member, moments after stepping off the aircraft, is surveilled by the airport's security camera system. Digital images of their faces are immediately imported into the robust security apparatus maintained by state intelligence agencies and integrated into the airport's comprehensive technical surveillance system. Facial recognition software, enabled by artificial intelligence, identifies all six team members as foreign nationals who had not yet visited Hanu and establishes a profile for each of them.

Their identities are confirmed, and their profiles cross-referenced and updated as the team processes through passport control. In addition, the team is required to provide fingerprints prior to clearing customs, allowing for a more complete profile of each person. This profile continues to build at the rental car desk as each driver's license and vehicle information is added to the centralized security database. As the team continues to travel together and interact, their profiles are linked by the AI algorithms of the surveillance system; the actions of one now influence the assessment of the others as well.

Upon arrival to the hotel, the team members begin using their personal devices via a 5G cell network connection. The IMEIs from their phones, the MAC addresses from their computers, as well as their individual device fingerprints allow the owner of the 5G network to develop specific digital profiles of each member of the team. Using geolocation, network architecture, and the hotel's record of each teammate's room location, each personal device and, therefore, its digital information is matched to the

individual's security profile. In minimal time, utilizing 5G interconnectivity and artificial intelligence to parse out key data, the host nation has a strikingly transparent view of the team.

Over the course of the next several days, the team conducts business as usual in the local community. They maintain a low physical profile while conducting meetings with the indigenous force they are assigned to train. They stroll leisurely on the beach while actually surveying a beach landing site. They go on runs across potential helicopter landing sites while becoming acquainted with the local area. At the conclusion of their work, the team enters the U.S. Embassy to submit their report via secure means to their superiors.

Unbeknownst to the team, each one of their activities was surveilled in incredible detail, enabled by the 5G network. Local traffic cameras augmented with facial recognition software identified the team on their way to rendezvous with the local forces. When the government security team cross-referenced this hit with cell phone metadata from local small, pico- and femto-cells distributed throughout the region, each team member's indigenous cell number was matched to their biometrics. Utilizing additional metadata—to include outgoing and incoming calls and text messages to key leaders of the indigenous force as well as the geolocation from each exploited device, the host nation was able to observe and develop a pattern of life on each team members' movements, continue to build intelligence profiles, and determine key areas of the team's focus. As a result, though not fully understanding the exact intent of the team's actions, the Hanuan intelligence service was able to determine that numerous open grassy areas, three particular beach locations, and two private residences were of significant importance to the team's mission.

Upon completion of their mission, the team checked out of the hotel, paid with their government credit cards with accounts linking each of them directly to the U.S. military. Believing they had successfully and

clandestinely completed their mission, the team proceeded to the airport. Arriving at the customs processing counter, the team's identities were once again confirmed by the integrated security system. However, this time, a security alert was triggered, and the team was detained. Faced with the aggregated meta- and surveillance data collected throughout the week, the team spent the next forty-eight hours with agents from the Hanu State Intelligence Division defending their actions.

Due to increased reliance on technology by special operations coupled with a 5G environment that can exploit this reliance, the modern operator is burdened by increased cyber and signature vulnerabilities. This vignette highlights the dangers of operating in a 5G adversarial environment without proper protective measures; military operations, daily pattern of life, and individual behaviors and associations can be developed at unprecedented speeds and with fidelity not yet seen. If weaponized, the data collected by the enemy may be able to predict a special operations team's movements, actions, and objectives—a significant problem for operational security and a risk to both the team and mission. Moreover, the level of surveillance and situational awareness of the team's activities could remove any plausible deniability, risking the safety of the team as well as incurring negative strategic impacts for U.S. interests. Whereas in previous conflicts special operations teams were able to manage their signatures more easily, a high-risk 5G network combined with advanced analysis tools presents unique and significant challenges in this realm.

B. SIGNATURE MANAGEMENT THREAT NEXUS

The factors illustrated in the Hanu vignette are each elements and components of the threat ecosystem. We addressed each of these elements in previous chapters; however, a look at the overlap of each threat element highlights some relationships worth exploring. Figure 8 portrays the four main elements of an adversarial data analysis framework combined to show these relationships converging within the signature management threat nexus.

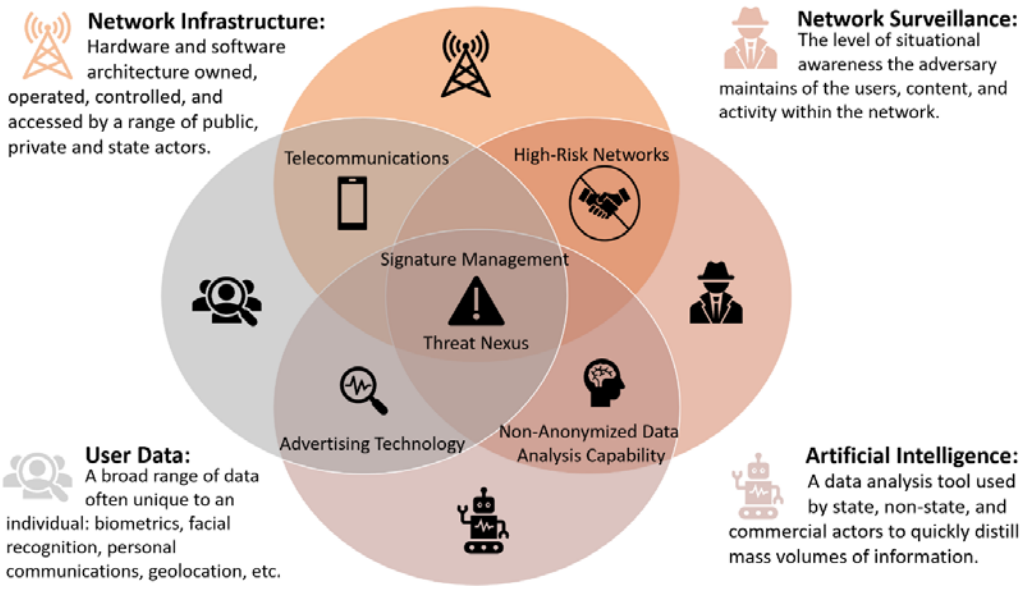


Figure 8. Signature Management Threat Nexus

The characteristics as well as the employment of the first two elements of the threat nexus, addressed in chapters II and III, are Network Infrastructure and User Data. Network Infrastructure includes the hardware and software architecture that is owned, operated, controlled, and accessed by a range of public, private, and state actors. The infrastructure connects end-users to data and vice-versa; this encompasses everything from the cellular architecture, personal devices, and the networked sensors that enable a smart city, to the virtual cellular network controls, and the software that enables device applications. User Data, on the other hand, includes the broad range of data unique to an individual: metadata, biometrics, facial recognition, traffic camera footage, passport control data, personal communications, shopping preferences, geolocation, etc. Accumulated information within a single device is simply a data set; however, the overlap of data transmitted and received within a network results in telecommunications. While singularly not a threat, telecommunication is a central component of the threat nexus.

The two remaining elements of the Signature Management Threat Nexus are Network Surveillance and Artificial Intelligence. Network Surveillance is the level of situational awareness the adversary maintains of the individual users as well as the content of their data and network activity. As discussed previously, it is suspected that China maintains a high level of control within their domestic networks and their reach has often

extended to the networks proliferated internationally by companies such as Huawei. We assess that non-anonymized user data as well as network information will be widely accessible to the Chinese government and other friendly and adversarial intelligence organizations. Artificial Intelligence is a useful surveillance analysis tool for state intelligence organizations. With the ability to distill massive amounts of data very quickly and to identify connections likely not observed by humans, AI is critical to the future of military and state intelligence. The combination of these two elements forms another central component of the threat nexus: Non-Anonymized Data Analysis Capability.

There are two other intersections of the main elements that combine in important ways. Advertising Technology is enabled by the combination of Artificial Intelligence and User Data; it is a common marketing analysis tool for commercial use in the exploitation of anonymized consumer data. Highlighted in chapters II and III, as the volume of data swells with the emergence of 5G technology, equally advanced artificial intelligence capabilities are growing to support the distillation of these data sets. Though generally used for commercial purposes, states can similarly apply analysis of non-anonymized data to meet national security objectives; the analysis of individual and group behaviors, preferences, and locations may provide an understanding of past and present behaviors while simultaneously providing the adversary with the tools to potentially predict future outcomes.

Finally, the last intersection—Network Infrastructure combined with Network Surveillance—results in a High-Risk Network. As discussed in Chapter III, these networks are subject to state-controlled surveillance and serve as a source of exploitable non-anonymized data. While Huawei sourced networks are an example of Chinese-controlled and surveilled high-risk networks, it should be assumed that this practice could be utilized by other state actors as well. Without sufficient countermeasures, users on this network should assume vulnerabilities to surveillance and privacy exist.

The convergence of these essential elements and components is the Signature Management Threat Nexus. Adversarial ability to access non-anonymized user data coupled with the capability to employ sophisticated AI algorithms may provide the ability to compromise the operational security of a mission. Not only could adversaries potentially

identify and monitor a specific team, but through weaponized advertising technology algorithms, it may also be possible for an adversary to predict the future behaviors, locations, or actions of a team.

C. SIGNATURE MANAGEMENT IMPLICATIONS OF 5G NETWORKS

The Signature Management Threat Nexus Model demonstrates how 5G telecommunications technology and its global proliferation will have numerous and significant impacts to small unit team operations throughout the world; however, managing signature within this environment may prove to be one of the most important challenges to overcome. Based on our research, we have prioritized three main implications that risk signature management in future operations:

Table 2. 5G Implications for Signature Management

1. High-risk 5G telecommunications networks will be the norm
2. 5G enables proliferation of unprecedented, ubiquitous technical surveillance capabilities
3. AI-driven intelligence analysis of surveilled and high-risk networks threatens signature management at a greater rate and with greater fidelity than pre-5G capabilities

High-risk 5G telecommunication networks will be the norm. Chinese and other adversarial high-risk 5G networks are prevalent throughout the world, particularly in regions where special operations forces operate. These high-risk networks—defined by the ability of a state or non-state actor to access non-anonymized user data—allow our adversaries a distinct advantage in the information warfare space, increasing the chance of non-anonymized surveillance of our teams' activities.

5G enables proliferation of unprecedented, ubiquitous technical surveillance capabilities. 5G networks provide a massive number of connections, unlocking the potential of the IoT. The IoT, often designed to connect consumer products or to integrate

community security infrastructures, can also actively and passively detect, process, and analyze data in near real-time. Regardless of the purpose, the IoT will establish novel and ubiquitous technical surveillance capabilities.

As AI capabilities mature, the information aggregated on surveilled and high-risk networks becomes more vulnerable to exploitation. The vast amounts of data becoming available, readily synthesized by hyper-enabled artificial intelligence, requires special operations forces to operate with more nuance and refined capabilities. Signatures that were once sufficiently managed may become liabilities in the future. AI-driven intelligence analysis of surveilled and high-risk networks threatens signature management at a greater rate and with greater fidelity than pre-5G capabilities.

The convergence of these implications presents novel challenges to our special operations forces. This new paradigm threatens to compromise operational security while complicating the ability of our forces to adequately manage signature through direct or deceptive means. However, we should not lose hope that signature management and age-old deception tactics are obsolete. Instead, we should look for opportunity in the same digital environment that has produced these risks; it may be possible that deception can be executed with significantly less effort and more rapidly than ever before.

The rapid growth of the information environment under the current 4G/LTE networks will only increase as the next generation 5G telecommunications technology is adopted. As a result, information warfare now rivals traditional conventional warfare.[159] Protecting and limiting the data available to the adversary will remain an important element of signature management. However, deception will also endure as an essential signature management tool as well. We are approaching an environment where instead of building an entire Ghost Army, an adept operator with a computer or simply a smart phone device may be able to execute sound deception. A keen operator at the edge, understanding both the environment and the perceptual and cognitive biases of his target, may be able to create ambiguity or doubt with remarkable efficiency.

---

[159] McFate, *The New Rules of War: Victory in the Age of Durable Disorder*, 8–9.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS

The emergence of 5G telecommunications technology promises to make fundamental changes in the way our world connects. Capabilities that were hypothetical until this point may soon be realized due to the increased bandwidth, capacity, and reduced latency of 5G architectures. While there are many reasons to welcome the benefits created by this new environment, the risks to our armed forces should be addressed thoughtfully and with caution. Particularly among our special operations forces, signature management is critical to military success; however, the proliferation of high-risk networks—many controlled by our adversaries—that unlock the capabilities of 5G connectivity and artificial intelligence will threaten special operations missions. Individual user data, data practices, physical signatures, and communications may simultaneously become aggregated, transmitted, analyzed, and actioned at unprecedented speeds. As was shown in Table 2 (repeated here for convenience) our research, thus far, has shown three primary implications.

Table 2. 5G Implications for Signature Management

1. High-risk 5G telecommunications networks will be the norm
2. 5G enables proliferation of unprecedented, ubiquitous technical surveillance capabilities
3. AI-driven intelligence analysis of surveilled and high-risk networks threatens signature management at a greater rate and with greater fidelity than pre-5G capabilities

Using the Threat Nexus Model and the implications that follow as a guide, there are several areas of interest to assist in the mitigation of each threat. Some items can be actioned immediately or prior to the widespread fielding of 5G technology while others will require a more long-term look, including research initiatives spread across various disciplines. The recommendations and research questions posed below are not comprehensive nor are they fully developed. The intention here is to provide opportunity

as well as inspiration for additional questions not posed by the authors. It is our hope that by identifying the elements and components that contribute to creating a signature management threat nexus, those charged with creating mitigation strategies may find a starting point to focus their efforts into one or more of these threat factors.

A. RECOMMENDATIONS

1. Immediate Action Opportunities

In the near-term, attention to end-user behaviors can protect the type and volume of user data present on the network. The critical process of protecting mission critical and personally identifiable information will remain a key tenet of managing signatures and protecting operational security, however, will become exponentially more difficult to execute. Because of this, continued cybersecurity, and personal data protection education of the force as well as integration of these elements into mission planning is essential.

a. RECOMMENDATION: Reduce User Data

Continue efforts to reduce the volume and sensitivity of data input onto public and private networks—this does not include government-sanctioned networks designed to support sensitive information, as there are proper security control mechanisms in place to protect the data. This recommendation extends to not only official government entities and associated activities but also to individual service members. Recognizing that our world is continuing to shift toward more and more data, individuals should still make mindful decisions relative to the type of personal data that is made accessible via the network, personal device applications, smart devices (i.e., fitness watches, networked home security devices, etc.), and other networked IoT hardware.

b. RECOMMENDATION: Protect User Data and Counter Surveillance

While many of the cybersecurity best practices are still vitally important during and after the transition to 5G technology, a recent Brookings Institution report highlighted that

data protection must adapt.[160] One key takeaway from the Brookings report as well as a Defense Innovation Board 5G study is that perimeter defense is no longer adequate; a zero-trust network approach will be required.[161] To do this, it will be necessary to procure, develop, and field robust encryption applications as well as other user identification and authorization strategies.[162] In the civilian sector, the industry continues to internally address how best to protect telecommunication network users from data compromise; however, the Brookings report suggests that much of the security burden remains with the user.[163] As military applications and networks continue to become more integrated into dual-use networks, it is imperative that the military removes the security burden from the end-user and instead develops a security framework that will protect critical data regardless of an end-user's technological sophistication.

c. RECOMMENDATION: Force Education on Compromised Networks and Advertising Technology

To prepare both our communicators as well as our operators to engage and operate in a high-risk network environment, training opportunities should be enhanced to address the security burdens they will bear. Topics should include but not be limited to:

- Zero-trust Network Approach
- Signature Management
- Advertising Technology Threats
- Encryption
- Cloud-based Network Operations and Management
- Mission Command/Decentralized Execution & Communication

d. RECOMMENDATION: Mission Planning for High Risk Networks

Mission planning tasks should include a comprehensive overview of the local telecommunications network. An assessment of the infrastructure, state control, likelihood

---

160 Tom Wheeler and David Simpson, "Why 5G Requires New Approaches to Cybersecurity," *Brookings*, September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

161 Wheeler and Simpson; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 29.

162 Macy Bayern, "How to Navigate Cybersecurity in a 5G World," *TechRepublic*, November 11, 2019, https://www.techrepublic.com/article/how-to-navigate-cybersecurity-in-a-5g-world/.

163 Wheeler and Simpson, "Why 5G Requires New Approaches to Cybersecurity."

of surveillance, vulnerabilities to data compromise, and other relevant factors should be utilized. This will allow planners and operators to identify overall risk to operational security, suitable signature management tools, TTPs, as well as appropriate hardware and software requirements for mission completion. As nations begin to transition to 5G, a flexible response to the types of technology fielded and strategies employed will be necessary and may require regionally dependent approaches.

2. Long-Term Opportunities

In the long-term, there are several lines of research that are necessary to fully understand the emerging battlespace as well as to identify techniques or technologies that may mitigate the risk of operating within regions that are characterized by high-risk networks. Current efforts by the United States to define a 5G National Security Strategy attempt to address the "risks to United States…national security during development and deployment of 5G infrastructure worldwide;" the following focus areas touch on a range of research questions that, if answered, may help navigate some of the national security and signature management obstacles presented by adversarial 5G networks around the world.[164]

a. RESEARCH: Network Infrastructure and High-Risk Networks

Security Vulnerability Assessment of 3GPP 5G Standards

The final international standards for 5G are still being finalized. Therefore, the United States has opportunity to influence the security protocols as well as other fundamental aspects of the 5G framework. In any case, a full security assessment of the 5G standards will be necessary for all end-users to understand what risks and vulnerabilities remain.

- Once finalized, what are the assessed security vulnerabilities of the established 3GPP Specification Set: 5G Standards? What are the standard security expectations?

---

[164] The White House, *National Strategy to Secure 5G of the United States of America* (Washington, DC: The White House, 2020), 1, https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

- What are the protocols to maintain physical and virtual security of the infrastructure?
- How does the implementation of these standards vary worldwide?
- How is cybersecurity best maintained to prevent bad actors from taking advantage of network virtualization controlled on publicly available operating systems utilizing common internet protocol language?
- How are IoT devices authenticated? Encrypted? What are the best practices to avoid backdoor network access via an unsecure IoT device?
- Through the procurement and controlled testing of an adversarial 5G network or discrete devices, what vulnerabilities and opportunities can be assessed?

b. RESEARCH: Network Infrastructure

Private Networks and Trusted Communication in High-Risk Networks

Private networks will be a fundamental element of future 5G networks for many reasons; self-driving cars, medical records, automated factories, and military applications are just a few. In theory, these networks ensure a secure medium upon which information can be shared, stored, and processed. When coupled with edge computing and catalyzed by 5G's low latency and increased bandwidth, these private networks may offer special operations teams a platform to operate away from the public architecture and hopefully, away from the scrutiny of a network operator. However, there are still several questions about the infrastructure required as well as the assurance of privacy that will need further evaluation.

- Are tactical, private 5G networks viable?
- What infrastructure, equipment, and manning are required to maintain tactical, private 5G networks?
- What level of assurance can be maintained?
- What level of trust or classification can be assured within a tactical, private 5G networks?

- Do tactical, private 5G networks assume additional signature management risks?
- Are trusted communications viable within a high-risk network?
- What level of trust or classification can be assured within a high-risk network?
- What additional end-to-end encryption, channel hardening, or other mechanisms are required to assure trusted communications?
- Do trusted or secure communications within a high-risk network assume additional signature management risks?

c. RESEARCH: Telecommunications and Compromised Networks

Edge Computing

The distributed nature of 5G networks also enables edge computing. Without the need to reach back to a centralized mainframe, critical analysis tools can be employed by end-users at the edge. This technique may reduce the required data traffic—and therefore digital signature—for in-field analysis. It may also enable teams to employ signature management tools to inject falsities, distractions, or other deception in near real-time.

- Does edge computing reduce the likelihood of data compromise?
- What capabilities may be enhanced by edge computing?
- Will edge computing reduce the likelihood of state-sponsored surveillance?
- Does edge computing reduce the required footprint of a SOF team?
- Can edge computing be utilized to inject falsities or a preferred signature into the network?

- What infrastructure, equipment, and manning are required to support edge computing?

d. RESEARCH: Telecommunications and Compromised Networks

Upskilling Via Virtual and Augmented Reality (VR/AR)

An opportunity presented within a 5G environment is the ability to employ upskilling by a team in the field. Due to the ultra-low latency and enhanced bandwidth, virtual and augmented reality could now enable virtual or remote team members to join an operation. Should a specialized skill be required, rather than bringing an additional person along and increasing the footprint and signature of an operation, a specialist could remotely guide, monitor, instruct, or *upskill* a special operations team on anything from field medicine to language interpretation to intelligence collection.

- Can SOF teams utilize VR/AR capabilities to employ upskilling and thus reduce the required footprint?
- What infrastructure, equipment, and manning are required to support VR/AR upskilling?
- What signature management benefits and risks are associated?

e. RESEARCH: Artificial Intelligence and Non-Anonymized Data Analysis Capability

Deception: Counter Non-Anonymized Data Analysis Capabilities

Generative Adversarial Networks (GANs) are supported by deep machine learning to actively deceive another AI network. Generally used to help AI networks learn, it is also possible to utilize a GAN to inject falsities to either disrupt analysis capabilities, flood an AI with false information, produce deep fakes, or simply obscure data. There may be opportunities to overcome several technical surveillance threats by utilizing a GAN for purposeful deception.

Other deception opportunities may include wearables to defeat biometric sensing or facial recognition. Additionally, physical alterations or camouflage may prove helpful in defeating early applications of AI-driven data analysis.

- Can a Generative Adversarial Network (GAN) be utilized to counter the non-anonymized data analysis capability of an adversary? Can a GAN reliably inject falsities or a preferred signature into the network?
- Can wearable IoT devices defeat biometric or facial recognition sensing?
- Can physical alterations or camouflage be utilized to defeat video surveillance?

There are likely many additional research opportunities not addressed above. As previously noted, the intent here is to simply inspire additional research questions and to provide a pathway to the relevant factors that contribute to signature management threats.

B. CONCLUSION

It is still too early to observe the full impact of 5G technology on societies, particularly how these capabilities will change the face of warfare. With a best attempt to anticipate a potential area of vulnerability, we have highlighted not only the technological change but also how these technologies can be weaponized. Militaries will have access to unprecedented volumes of data streaming in at near real-time for analysis. Sophisticated AI tools and behavioral analysis algorithms currently employed by commercial entities can rapidly and accurately distill that data into actionable intelligence. Current location, battlefield characterization, and predictive behavior assessment may soon easily be generated by the rapid analysis of seemingly unrelated, aggregated data.

As 5G networks are proliferated around the world, special attention should be paid to which entities own, operate, and access the infrastructure as well as the data. Authoritarian regimes that enjoy unfettered access to non-anonymized user data and network information are likely to use this capability to control and influence their own people as well as maintain situational awareness of military and state intelligence interests.

SOF operations within regions assessed to have high-risk networks without some level of mitigation may be in danger of compromising their forces and their mission. Though the United States may have been caught on their heels in this respect, we should not be discouraged in our ability to overcome and to mitigate these risks.

Now is a unique yet narrow window of opportunity to actively engage with the challenges and opportunities within this paradigm, to innovate solutions and drive the emerging design of an environment that is not yet determined, and to truly adapt to tomorrow's fight rather than prepare to fight the last war better. Our adversaries have embraced this call-to-arms, yet there is time—though fleeting—to learn from, to adapt to, and to control this environment. It is therefore crucial that leaders develop strategies to protect the signature management of our teams; these strategies should address the risks in telecommunications, high-risk networks, advertising technology, and non-anonymized data analysis. The strategies should strive for defensive capabilities yet also seek opportunity for advantage. Effective implementation will require immediate action paired with intelligent feedback as well as long term investment in public and private research lines of effort. Ignoring any one of the essential elements and components that threaten signature management will leave our forces insufficiently protected and our national security at risk.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. A SURVEY OF 5G TECHNOLOGY ADVANCEMENTS

The allocation of new radio wavelength bands, alterations to the cellular base station architecture and network control, as well as the design of smart and directional antennae are only a few of the technical challenges 5G innovators will face. While the following sections do not provide an exhaustive survey of the emerging 5G technology, the key adaptations that will affect SOF operations or have signature management implications are addressed.

A. WAVEFORMS: A DEBATE OVER LOW, MEDIUM, AND HIGH BANDS

The debate over which frequency bands will dominate 5G is still open, however, it is likely that the network will depend upon frequencies in the low, medium, and high bands. Aside from meeting the consumer and industry demands for faster, more capable cellular networks, 5G technology promises to meet another growing challenge—bandwidth. Currently, wireless technology operates primarily in low frequency bands—generally between 3kHz and 3GHz.[165] These frequency bands—shown in Figures 9 and 10—traditionally offered reliable propagation characteristics and had plenty of data carrying capacity.[166] Over time, however, these bands have become congested and continue to host 3G and 4G cellular networks, Wi-Fi, WiMAX, L-band, C-band and S-band satellite communication, GPS, as well as several other RF-based technologies.[167]

[165] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1618.

[166] Agiwal, Roy, and Saxena, 1618.

[167] Sunny Classroom, "5G Cellular Networks"; Gupta and Jha, "A Survey of 5G Network," 1207.

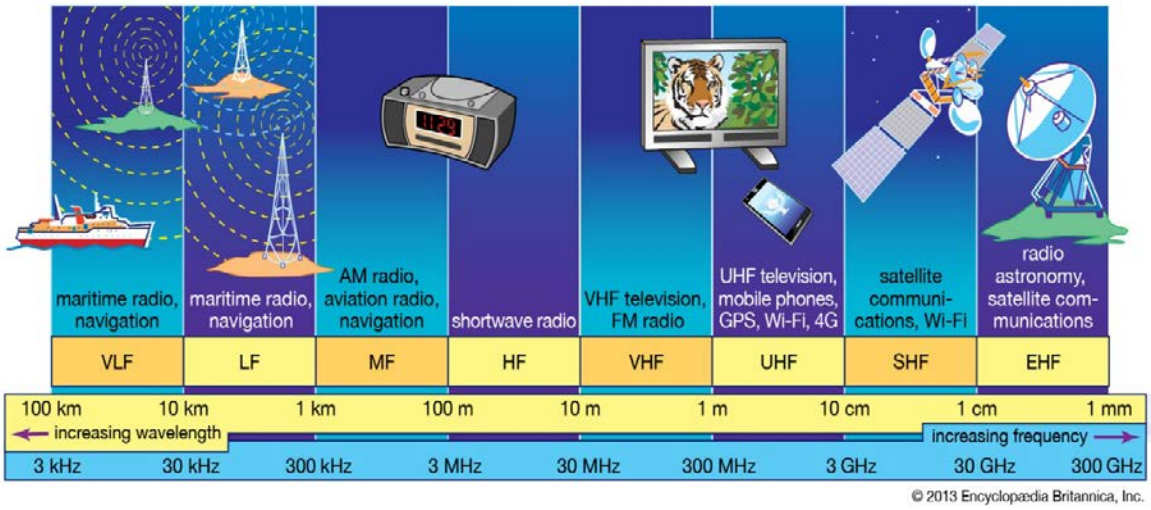


Figure 9. Commercially Exploited Bands of the Radio-Frequency Spectrum[168]

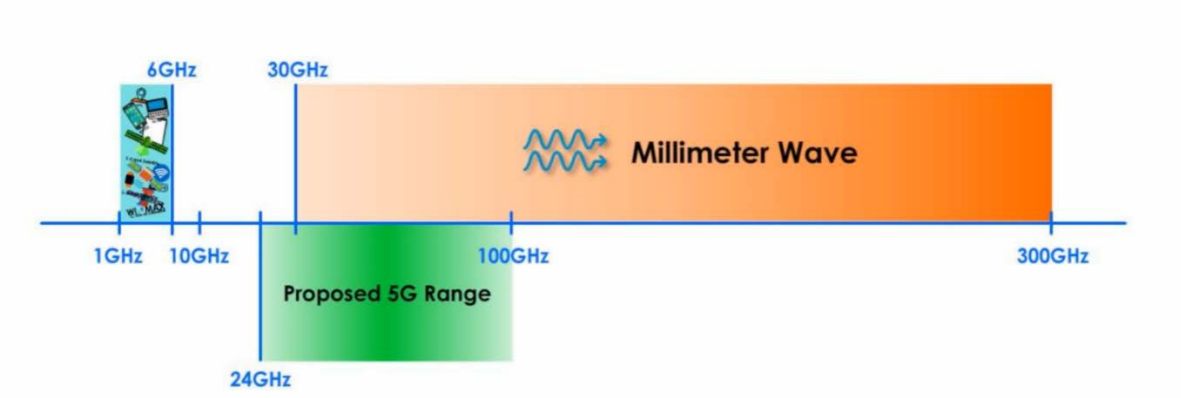


Figure 10. Proposed 5G Radio-Frequency Band[169]

As more wireless technology is added to the network, the already overcrowded frequency bands risk reducing overall capability and quality of experience. In response, scientists and industry leaders are exploring other frequency bands in addition to techniques for more efficient use of current bands. Low, medium, and high bands are under examination and each offer distinct opportunities as well as drawbacks (Figure 2, reprinted

168 Source: "Radio-Frequency Spectrum."

169 Source: Sunny Classroom, "5G Cellular Networks."

here for convenience, illustrates these characteristics).[170] In fact, companies such as Huawei, Verizon, and Ericsson have already begun the acquisition and development of these bands.[171] It is important to note, that while each band has some unique characteristics, the high frequency bands currently under development are of interest mainly due to the available space to expand; had the high bands been used for the original telecommunications generations, we would now be expanding into the low bands.[172]

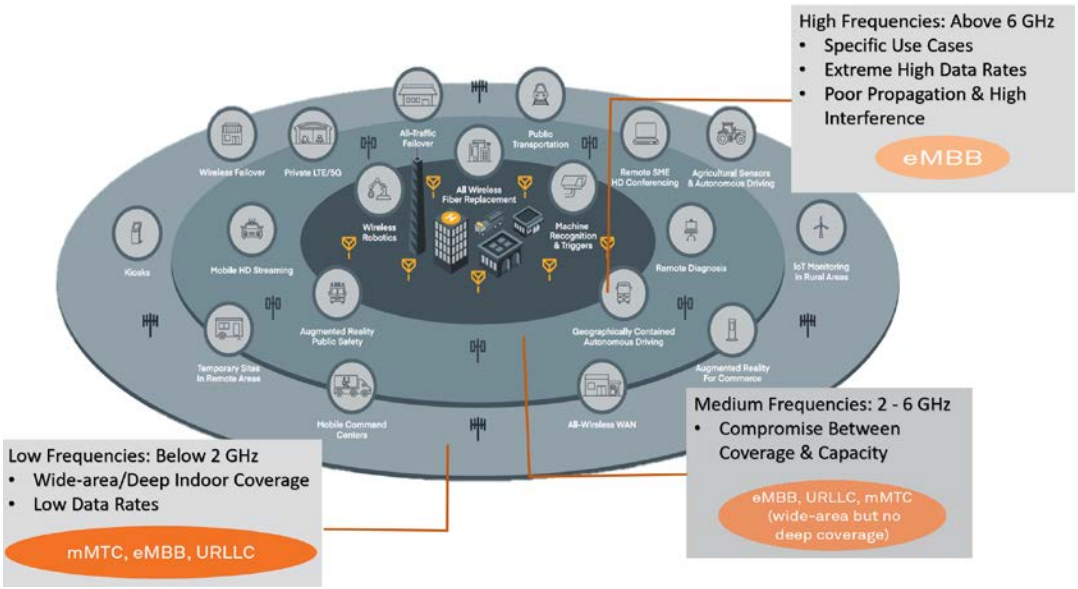


Figure 2. Multi-layer Frequency Overlay on 5G Use-Cases[173]

Low Bands. At the low end of the RF bands, frequencies less than 2 GHz show promise for wide-area coverage and deep indoor coverage for a range of capabilities. Although the data rates are significantly lower than medium and high frequencies due to

---

170 "Public Policy Position: 5G Spectrum," 6; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 12.

171 "Public Policy Position: 5G Spectrum," 10–12; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 12.

172 Sue Marek, "Low-Band, Mid-Band or High-Band—Why Spectrum Bands Matter in a 5G World," *Futurithmic*, February 11, 2020, https://www.futurithmic.com/2020/02/11/why-spectrum-bands-matter-in-a-5g-world/. For a more detailed discussion relative to waveform characteristics, see the Appendix.

173 Adapted from "Public Policy Position: 5G Spectrum," 6; Cradlepoint 5G Strategy Group, *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*, 7–8.

the congested bands, less demanding applications such as passive sensors, IoT integration, and even some massive machine type communications (mMTC) and ultra-reliable latency communications (URLLC) capabilities may benefit from the extended range and reduction of environmental interference within the low band. Much of the infrastructure, hardware, and devices currently deployed worldwide already support these frequency bands and these bands extend the range of certain 5G capabilities; however, limitations in data capacity and frequency crowding restrict the effectiveness of these bands.[174] As such, the use of this band will likely be restrained in the future.

High Bands. On the other side of the spectrum, high frequency bands are generally less crowded, allowing for scientists to explore the mmWave bands, generally between 3–300 GHz.[175] These frequencies—named so because the physical wavelength of these frequencies are measured in millimeters vice the traditional wireless frequencies that are measured in meters or kilometers—promise extremely high data rates.[176] The high bands identified for 5G (24-100GHz) are largely untapped, supporting wide bandwidth availability enabling very high data rates.[177]

These frequencies, however, suffer from drawbacks in undesirable propagation characteristics and increased environmental interference. This disadvantage drives mmWave to exist as a largely line-of-sight capability, somewhat relieved by some clever engineering and smart antenna technology. Though mmWave does not have the range and penetration capabilities of low frequency bands, the waveform requires a much smaller antenna, allowing a single cell station to support 10–100 times more antennae.[178] As a result, a much denser antenna architecture is utilized, integrating multiple sizes of cellular

---

174 "Public Policy Position: 5G Spectrum," 6; Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 10.

175 Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1618.

176 Cradlepoint 5G Strategy Group, *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*, 7.

177 Sunny Classroom, "5G Cellular Networks."

178 Erik G. Larsson et al., "Massive MIMO for next Generation Wireless Systems," *IEEE Communications Magazine* 52, no. 2 (February 2014): 187, https://doi.org/10.1109/MCOM.2014.6736761.

access nodes and is comprised of thousands of nested small-, micro-, pico- and femto-cells tightly distributed throughout a city. The density of the antennae should eliminate coverage gaps that manifest due to interference and undesirable propagation characteristics of the high band.[179] There is still much to be discovered, designed, and implemented within the mmWave bands, however, if estimations hold, the true leaps in capability that 5G promises can only be realized with the integration of these higher bands.

Medium Bands. The medium bands, often referred to as the sub-6 GHz bands, have shown early success not only overcoming several of the shortfalls of the low and high bands, but also share many of the advantages of each band. Although upgrades to devices and some infrastructure are still required for this band, the advantages and disadvantages in coverage, capacity, and latency seem to be more balanced within this band. One of the greatest advantages of the sub-6 5G bands is its ability to reasonably propagate and penetrate obstacles while also supporting a much greater capacity and very low latency as compared to current 4G/LTE networks.[180] In fact, the majority of carriers throughout the world, including Huawei/ZTE, T-Mobile, and Ericsson, who are early implementors of 5G networks are operating or testing within this mid-band.[181]

Demonstrated in Figure 11, a Signal Propagation Loss and Terrain (SPLAT) chart of potential 5G wavelengths, urban landscapes have a significant effect on mmWave (28 GHz) and sub-6 GHz (3.4 GHz) frequencies.[182] Users in blue would experience 100Mbps of speed compared to users in red achieving up to 1 Gbps.[183] The sub-6 propagation travels over two and half times as far as the mmWave while accommodating similar data rates and speeds. Many experts believe that these advantages will cement sub-6 bands as the primary

---

[179] Sunny Classroom, "5G Cellular Networks"; "What Is 5G? Understanding the Next-Gen Wireless System Set to Enable Our Connected Future," January 23, 2019, https://www.cbinsights.com/research/5g-next-gen-wireless-system/; Agiwal, Saxena, and Roy, "Towards Connected Living: 5G Enabled Internet of Things (IoT)," 196.

[180] "What Is 5G?"; Gilbert, "Spectrum for 5G Will Ensure Investment in Africa."

[181] "Public Policy Position: 5G Spectrum," 10; Morris, "Ericsson Hails 5G Test on Another Sub-6 GHz Band"; "Built for the 5G Future."

[182] Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 9.

[183] Medin and Louie, 9.

frequencies for emerging networks.[184] There are others, however, that believe sub-6 bands are simply a transitional band, enabling the leap to mmWave 5G following further research, testing and fielding.[185] In either scenario, it seems that the architecture will comprise of some combination of each band.

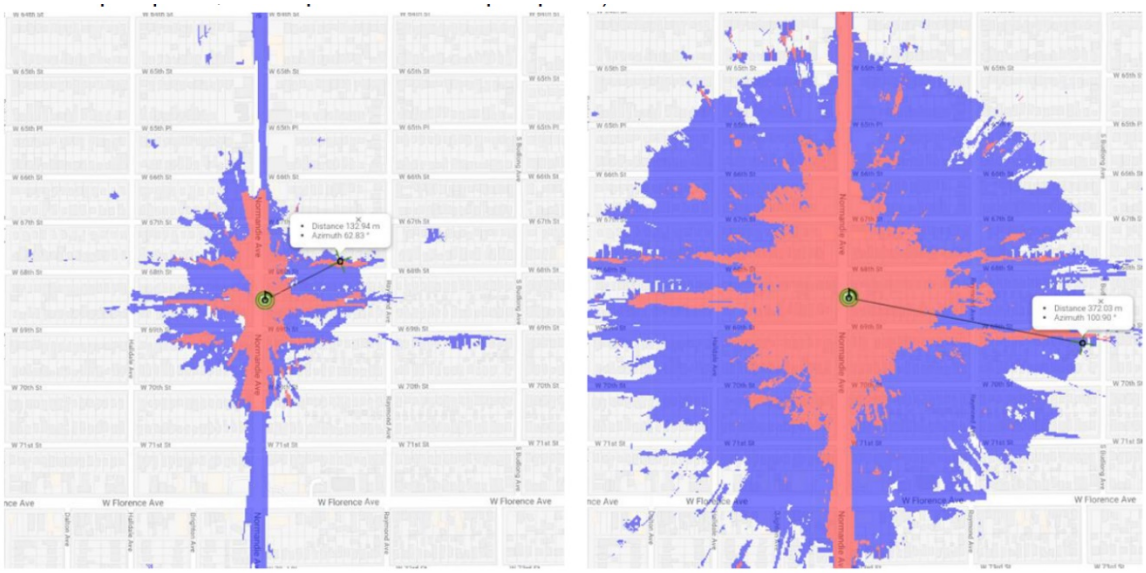


Figure 11. "SPLAT" Chart of mmWave Propagation (left) vs. Sub-6 Propagation (right)[186]

Multi-band Approach. While each band has its own strengths and weaknesses, it is likely that each one will play an important role in enabling future 5G networks. While it is likely that the medium band will do the majority of the heavy lifting for now, there are functions that this bands would be incapable of executing—enhanced mobile broadband requiring extremely high data rates coupled with low latency—or would be inappropriate for—IoT systems that do not demand high data or latency characteristics. It is in these

[184] Medin and Louie, 10; "Public Policy Position: 5G Spectrum," 5.

[185] "Key Breakthroughs to Drive a Fast and Smooth Transition to 5G Standalone," August 2, 2019, https://www.qualcomm.com/news/onq/2019/08/19/key-breakthroughs-drive-fast-and-smooth-transition-5g-standalone.

[186] Source: Medin and Louie, *The 5G Ecosystem: Risks & Opportunities for DOD*, 9.

instances that the high- or low-bands would be more appropriate. The trade-offs associated with each band are summarized below in a reprint of Figure 3; balancing capacity and latency with wide-area coverage and building penetration will require a blend of each band. And until the science, technology, and infrastructure catches up, it may be some time until the full benefits of mmWave are seen.[187]

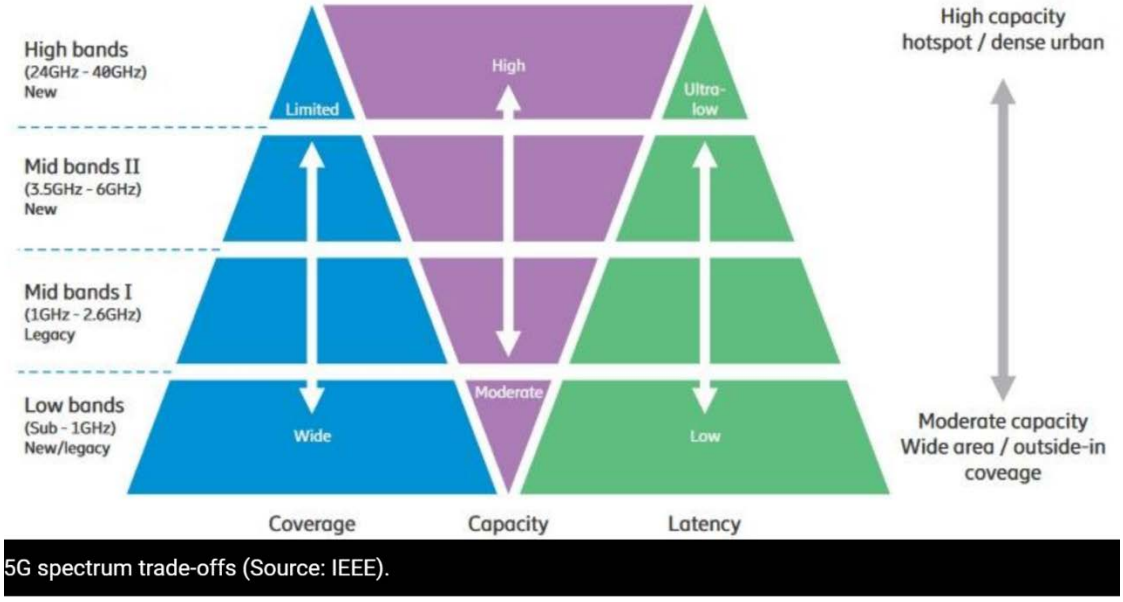


Figure 3. 5G Spectrum Trade-Offs[188]

B. ARCHITECTURE: DENSE, USER-CENTRIC HYBRID AND STANDALONE NETWORKS

The current radio access network (RAN) architecture is base station centric; systematically placed macro base stations, each responsible for a hexagonal footprint, are linked to mobile switching centers (MSC) that direct voice and data traffic within the network.[189] This system works well within the currently utilized radio frequency (RF) due to efficient area coverage and frequency reuse as well as the propagation characteristics of

[187] personal communication, February 18, 2020.

[188] Source: Gilbert, "Spectrum for 5G Will Ensure Investment in Africa."

[189] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1620.

the current bands.[190] Though geography and other environmental variations will alter the architecture requirements, traditional telecommunication networks are largely regular shapes and the architecture is centralized around the base station. Due to a combination of capabilities and constraints of 5G standalone and legacy/5G hybrid networks, traditional cell architecture is no longer sufficient. Figure 12 shows the evolution that will occur from a base station centric network to the emerging user centric network.[191]

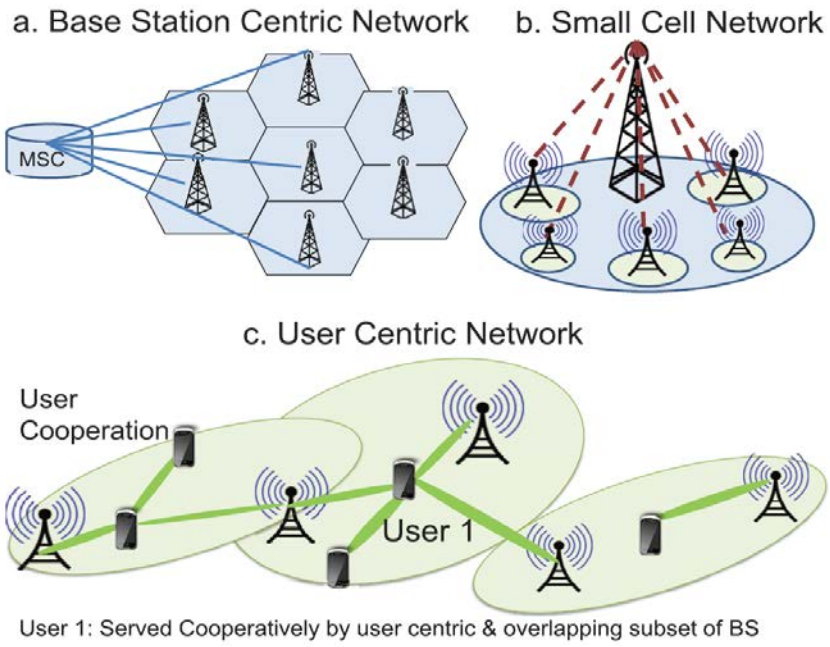


Figure 12. Shift from Base Station Centric to User Centric Architecture[192]

The frequency bands identified for 5G telecommunications technology paired with advances in waveform and end-device technology will introduce key differences in how the network architecture will likely be designed. As previously discussed, three distinct

[190] Konstantinos B. Baltzis, "Hexagonal vs Circular Cell Shape: A Comparative Analysis and Evaluation of the Two Popular Modeling Approximations," in *Cellular Networks*, ed. Agassi Melikov (Rijeka: IntechOpen, 2011), 104, https://doi.org/10.5772/14851.

[191] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1620.

[192] Source: Agiwal, Roy, and Saxena, 1620.

bands (low, medium, and high) have been identified to potentially fulfill the requirements of 5G capabilities; however, the medium band (often referred to as sub-6) and high band (often referred to as mmWave) will drive many of the network advancements. Sub-6 bands, though generally higher frequency than the current 4G/LTE bands, are similar to our current capabilities, though they do offer some exciting boosts to speed, capacity, and connectivity. Alternatively, mmWave bands promise to fully realize the desired upgrades to capabilities despite drawbacks to the decreased propagation characteristics and increased interference of the mmWaves. To overcome the negative wave characteristics, future 5G networks will need to be much denser—to include the proliferation of macro, small, micro, pico, and femto cell deployments—but also more user centric.[193] Illustrated in Figure 13, this transition to 5G will manifest itself in hybrid and standalone networks.[194]

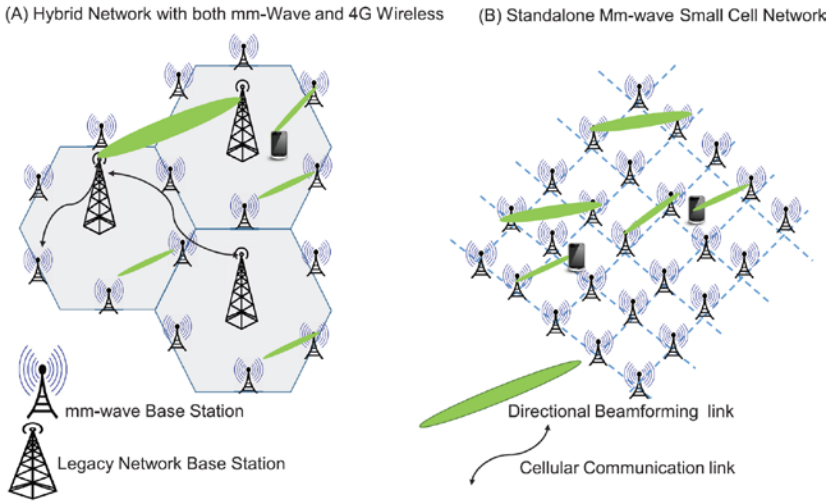


Figure 13. Standalone and Hybrid mmWave Network Architecture[195]

These network architectures are not mutually exclusive. In fact, it is likely that hybrid and standalone architectures will provide discrete benefits to different regions based on the unique needs of each community. Most regions throughout the world and particularly large cities already have well-established 4G/LTE infrastructures built into

193 Agiwal, Roy, and Saxena, 1621.

194 Agiwal, Roy, and Saxena, 1621.

195 Source: Agiwal, Roy, and Saxena, 1621.

their dense urban spaces. The transition to 5G will require a massive amount of bandwidth in an area plagued by signal interference; a hybrid network can bolt onto the existing infrastructure and still take advantage of the higher frequency bands, emerging smart antenna technology, and distributed networks enabled by edge computing.

Alternatively, purposefully planned smart cities such as the Konza Technopolis in Kenya could benefit from standalone, heterogenous 5G networks.[196] Although this project has stalled, the concept of Konza may be duplicated in the future due to infrastructure advantages; without competing legacy infrastructure constraints, a smart city can organically grow on a standalone 5G architecture.[197] In either case, each network design will likely benefit from a Network Functions Virtualization (NFV)-based control and maintenance of RAN functions. In an NFV, physical, localized maintenance and control functions are replaced by a central, cloud-based tool capable of remotely monitoring, maintaining, updating, or fixing particular cells or entire networks. This will reduce operating costs via the deployment of generic, programmable hardware and centralizing the expensive network "brains."[198]

Utilizing several types of access technologies (e.g., cellular, Wi-Fi), multiple radio access technology (Multi-RAT)—shown in Figure 14—designs allow each unique architecture to connect into a unified framework and will be the backbone of emerging 5G and IoT architectures.[199] Supporting the growing demand of smart cities, autonomous vehicles, and other IoT wireless capabilities, the network will be empowered by a wide range of cell stations and access points densely populated to provide massive amounts of data and super low latency to an incredible number of devices.[200]

---

196 "Konza Technopolis: Smart City," 2019, https://www.konza.go.ke/smart-city/.

197 "Konza Technopolis: Master Plan," 2019, https://www.konza.go.ke/master-plan/.

198 personal communication, February 18, 2020; personal communication, February 27, 2020.

199 Agiwal, Saxena, and Roy, "Towards Connected Living: 5G Enabled Internet of Things (IoT)," 192.

200 Agyapong et al., "Design Considerations for a 5G Network Architecture," 4–5; Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1627.

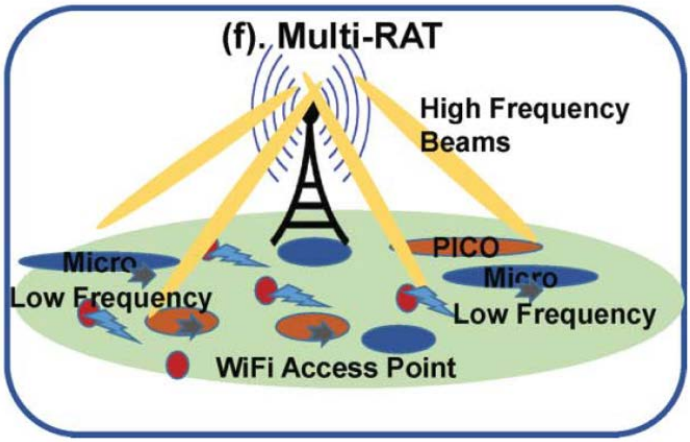


Figure 14. Multi-RAT Integration[201]

C. ANTENNAE: MMIMO, SPATIAL DIVERSITY/MULTIPLEXING AND BEAMFORMING

A blended low, medium, and high band approach to 5G architecture will be enabled not only by the user centric and Multi-Rat architectures discussed previously, but also by advances in antenna technology. The shorter, high frequency waves proposed for the medium and high bands will require closer, line-of-sight signals to maintain a connection. However, the RF signal requires a much smaller antenna, allowing for many more antennae within a single cell and an increased number of connections within a geographic area. A dense layout of antennae combined with massive multiple input multiple output (mMIMO) technology and nimble antenna pathways to maintain adequate line-of-sight signal strength will ensure the incredible number of connections are supported.[202]

mMIMO. For some time, networks have depended on both cells and devices to have MIMO capabilities; in other words, each end utilizes multiple antennae in conjunction with sophisticated algorithms to determine where the energy of the wave is focused as well as how the data is mapped by the endpoint.[203] The compact size of sub-6 GHz and mmWave

---

[201] Source: Agiwal, Saxena, and Roy, "Towards Connected Living: 5G Enabled Internet of Things (IoT)," 195.

[202] Agiwal, Roy, and Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," 1621.

[203] "How 5G Massive MIMO Transforms Your Mobile Experiences."

antennae alone facilitate a greater number of connections, however, via spatial diversity, spatial multiplexing and beamforming techniques, the capabilities of mMIMO will be more important for the efficient use of the waveforms and the space they operate in.

Spatial Diversity and Multiplexing. Within a very dense network, it is likely that signals will not only interfere with the environment but may also interfere with each other. Spatial diversity utilizes unique signal pathways to deconflict signals.[204] Allowing for additional capacity within the network, spatial multiplexing (illustrated in Figure 15) is a technique which allows a single device to send multiple messages simultaneously along deconflicted pathways; rather than limiting transmission to a single pipeline, multiple pipelines are available, and the volume of data transferred is significantly increased.[205]

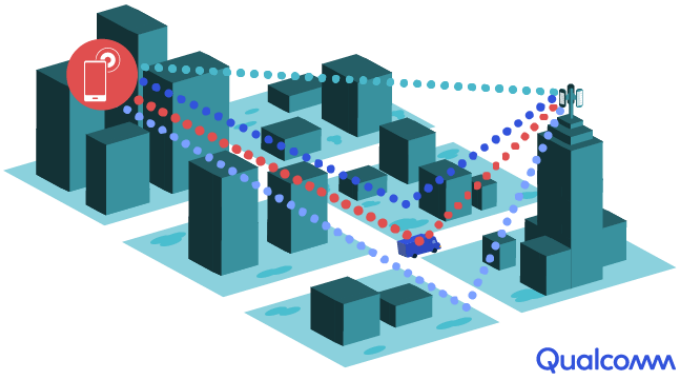


Figure 15. Spatial Multiplexing[206]

Beamforming. Beamforming is a technique linked to spatial diversity. Analogous to transitioning from a lightbulb to a laser beam, this method focuses the RF signal in three dimensions between base stations to end-devices, allowing for a narrower signal and deconfliction within the spectrum.[207] Traditional base stations emit in sectors, roughly in thirds of a sphere; beamforming will instead transmit directional signals based on the

[204] Qualcomm.

[205] Qualcomm.

[206] Source: Qualcomm.

[207] Qualcomm.

relative geolocation of each device.[208] As Figure 16 demonstrates, these devices are often mobile, yet beamforming allows for a focused signal to dynamically track and support each device.[209]

Figure 16. 3D Beamforming[210]

[208] Qualcomm.

[209] Qualcomm.

[210] Source: Qualcomm.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agiwal, Mamta, Abhishek Roy, and Navrati Saxena. “Next Generation 5G Wireless Networks: A Comprehensive Survey.” *IEEE Communications Surveys & Tutorials* 18, no. 3 (2016): 1617–55.

Agiwal, Mamta, Navrati Saxena, and Abhishek Roy. “Towards Connected Living: 5G Enabled Internet of Things (IoT).” *IETE Technical Review* 36, no. 2 (March 4, 2019): 190–202. https://doi.org/10.1080/02564602.2018.1444516.

Agyapong, Patrick, Mikio Iwamura, Dirk Staehle, Wolfgang Kiess, and Anass Benjebbour. “Design Considerations for a 5G Network Architecture.” *IEEE Communications Magazine* 52, no. 11 (November 2014): 65–75. https://doi.org/10.1109/MCOM.2014.6957145.

Almond, Kyle. “A Rare Look Inside Huawei, China’s Tech Giant.” *CNN*, May 2019, sec. Business. https://www.cnn.com/interactive/2019/05/business/huawei-cnnphotos/index.html.

Alsever, Jennifer. “How 5G Will Fundamentally Change Everything You Know About Mobile Computing: From Farms to Phones.” *Inc. Magazine*, February 2020. https://www.inc.com/magazine/202002/jennifer-alsever/5g-wireless-network-broadband-high-speed-gigabit-technology.html.

Andersson, Kent. “On the Military Utility of Spectral Design in Signature Management: A Systems Approach.” PhD diss., National Defence University, 2018. https://www.doria.fi/bitstream/handle/10024/152611/Andersson_thesis_full%20%28web%29.pdf?sequence=1&isAllowed=y.

Araya, Daniel. “Huawei’s 5G Dominance in the Post-American World.” *Forbes*, April 5, 2019. https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/.

Atallah, Mikhail J., and Nicholas J. Hopper. “Erratum to: Privacy Enhancing Technologies.” In *Privacy Enhancing Technologies*, edited by Mikhail J. Atallah and Nicholas J. Hopper, 6205:E1–E1. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017. http://link.springer.com/10.1007/978-3-642-14527-8_17.

Atlantic Council. “My Way or the Huawei: 5G at the Center of US-China Strategic Competition,” July 23, 2019. https://www.atlanticcouncil.org/blogs/econographics/my-way-or-the-huawei-5g-at-the-center-of-us-china-strategic-competition/.

Baltzis, Konstantinos B. “Hexagonal vs Circular Cell Shape: A Comparative Analysis and Evaluation of the Two Popular Modeling Approximations.” In *Cellular Networks*, edited by Agassi Melikov. Rijeka: IntechOpen, 2011. https://doi.org/10.5772/14851.

Bayern, Macy. “How to Navigate Cybersecurity in a 5G World.” *TechRepublic*, November 11, 2019. https://www.techrepublic.com/article/how-to-navigate-cybersecurity-in-a-5g-world/.

BBC Click. “Inside Huawei and 5G.” Video, 6:14, May 8, 2019. https://www.youtube.com/watch?v=_8HqbPBRiS4.

Bell, J. Bowyer. “Toward a Theory of Deception.” *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (April 2003): 244–79. https://doi.org/10.1080/08850600390198742.

Blumenthal, Eli. “AT&T Bolsters 5G Network with New Low-Band and Millimeter-Wave Markets.” *CNET*, December 30, 2019. https://www.cnet.com/news/at-t-bolsters-5g-network-with-new-low-band-and-millimeter-wave-markets/.

Broughton, Mathew. “The Future Is 5G: How New Mobile Tech Will Take Advertising into the 5th Generation.” *Exchange Wire* (blog), April 29, 2019. https://www.exchangewire.com/blog/2019/04/29/the-future-is-5g-how-new-mobile-tech-will-take-advertising-into-a-fifth-dimension/.

Bryant, Steven. “The Dangers of an Over-Reliance on Technology.” Master’s thesis, Joint Advanced Warfighting School, 2011.

Buckley, Chris, and Paul Mozur. “How China Uses High-Tech Surveillance to Subdue Minorities.” *The New York Times*, May 22, 2019, sec. World. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

“Cambodia Profile.” *BBC News*, July 9, 2014, sec. Asia. https://www.bbc.com/news/world-asia-pacific-13006542.

Campbell, Charlie. “The Entire System Is Designed to Suppress Us: What the Chinese Surveillance State Means for the Rest of the World.” *Time*, November 21, 2019. https://time.com/5735411/china-surveillance-privacy-issues/.

CB Insights Research. “5G & the Future of Connectivity: 20 Industries the Tech Could Transform,” March 19, 2019. https://www.cbinsights.com/research/5g-technology-disrupting-industries/.

———. “What Is 5G? Understanding the Next-Gen Wireless System Set to Enable Our Connected Future,” January 23, 2019. https://www.cbinsights.com/research/5g-next-gen-wireless-system/.

"China: Digital Silk Road Will Boost China's ICT Sector." *Oxford Analytica Daily Brief Service*, January 22, 2018. http://search.proquest.com/docview/1989534760/.

"China: OBOR Will Follow Opportunities, Not Blueprint." *Oxford Analytica Daily Brief Service*, June 21, 2017. http://search.proquest.com/docview/1913904392?rfr_id=info%3Axri%2Fsid%3Aprimo.

Chokshi, Niraj. "How Surveillance Cameras Could Be Weaponized with A.I." *The New York Times*, June 13, 2019, sec. U.S. https://www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html.

Coyle, Keven P. "U.S. Military Technology Dependence: The Hidden Vulnerability to National Security." Master's thesis, Joint Advanced Warfighting School, 2016.

Cradlepoint 5G Strategy Group. *The 5G for Business Guidebook: A Guide to Understanding and Exploring the Pathway to 5G*. 2nd ed. Boise, ID: Cradlepoint, 2020. www.cradlepoint.com/5G.

Crawford, Robert J. "Reinterpreting the Japanese Economic Miracle." *Harvard Business Review*, January 1, 1998. https://hbr.org/1998/01/reinterpreting-the-japanese-economic-miracle.

Dinucci, Manlio. "The Hidden Military Use of 5G Technology." *Telesurtv*, December 21, 2019, sec. Opinion. https://www.telesurenglish.net/opinion/The-Hidden-Military-Use-of-5G-Technology-20191221-0006.html.

"Ericsson Mobility Report." Stockholm, Sweden: Ericsson, June 2018. https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-june-2018.pdf.

"Ericsson Sees Light in Tunnel." *The Australian Business Review*. March 17, 2017. https://www.theaustralian.com.au/business/technology/ericsson-sees-light-at-end-of-tunnel-thanks-to-telstra-tieup/news-story/d1971a894cb2d1990d3dd29f3b0203ac.

Estrada-Jiménez, José, Javier Parra-Arnau, Ana Rodríguez-Hoyos, and Jordi Forné. "Online Advertising: Analysis of Privacy Threats and Protection Approaches." *Computer Communications* 100 (March 1, 2017): 32–51. https://doi.org/10.1016/j.comcom.2016.12.016.

Feldstein, Steven. "The Global Expansion of AI Surveillance." Washington, DC: Carnegie Endowment for International Peace, September 17, 2019. https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

Feng, Emily, and Amy Cheng. “China’s Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts to Ban It.” *National Public Radio*, October 24, 2019, sec. World. https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it.

Gilbert, Paula. “Spectrum for 5G Will Ensure Investment in Africa.” *ITWeb*, November 20, 2018, sec. Telecom. https://www.itweb.co.za/content/dgp45qaGWaD7X9l8.

Gilpin, Robert. “Three Ideologies of Political Economy.” In *The Political Economy of International Relations.* Princeton, N.J.: Princeton University Press, 1987.

Gilpin, Robert., and Jean Gilpin. *Global Political Economy: Understanding the International Economic Order*. *Global Political Economy: Understanding the International Economic Order*. Princeton: Princeton University Press, 2001.

Gross, Terry, and Dave Davies. “How Tech Companies Track Your Every Move and Put Your Data Up for Sale.” *Fresh Air*, July 31, 2019. https://www.npr.org/2019/07/31/746878763/how-tech-companies-track-your-every-move-and-put-your-data-up-for-sale.

Grover, Vandita. “7 Ways 5G Will Help Advertising Evolve in 2019.” *Martech Advisor* (blog), April 5, 2019. https://www.martechadvisor.com/articles/ads/7-ways-5g-advertising-evolve-2019/.

Gupta, A., and R. K. Jha. “A Survey of 5G Network: Architecture and Emerging Technologies.” *IEEE Access* 3 (2015): 1206–32. https://doi.org/10.1109/ACCESS.2015.2461602.

Hammes, T. X. “Technology Converges; Non-State Actors Benefit.” *Governance in an Emerging New World*, Winter, no. 319 (February 25, 2019). https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

Huawei. “Video Surveillance as the Foundation of ‘Safe City’ in Kenya,” 2019. https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya.

Husson, Thomas. “Mobile’s Untapped Value Is in Contextual Data.” *Forrester* (blog), October 27, 2014. https://go.forrester.com/blogs/14-10-27-mobiles_untapped_value_is_in_contextual_data/.

Hwee, Wee Kee, and Amelia Santos Paulino. “ASEAN Investment Report 2019.” Jakarta, Indonesia: ASEAN Secretariat and United Nations Conference on Trade and Development, 2019. https://unctad.org/en/PublicationsLibrary/unctad_asean_air2019d1.pdf.

IEEE Future Networks: Enabling 5G and Beyond. “Standards,” 2020. https://futurenetworks.ieee.org/standards.

Jain, Shruti. “Mobile VNI Forecast 2017–2022: 5G Emerges and Is Here to Stay!!” *Cisco Blogs* (blog), February 26, 2019. https://blogs.cisco.com/sp/mobile-vni-forecast-2017-2022-5g-emerges.

Joint Chiefs of Staff. *Joint Publication 3-13.4, Military Deception*. Joint Chiefs of Staff, 2012. https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.

Kirkpatrick, David. “Why Just-In-Time Trumps Real-Time for Marketing Efficiency.” *Marketing Dive*, October 17, 2016. https://www.marketingdive.com/news/why-just-in-time-trumps-real-time-for-marketing-efficiency/422353/.

Konza Technopolis. “Konza Technopolis: Master Plan,” 2019. https://www.konza.go.ke/master-plan/.

———. “Konza Technopolis: Smart City,” 2019. https://www.konza.go.ke/smart-city/.

Larsson, Erik G., Ove Edfors, Fredrik Tufvesson, and Thomas L. Marzetta. “Massive MIMO for next Generation Wireless Systems.” *IEEE Communications Magazine* 52, no. 2 (February 2014): 186–95. https://doi.org/10.1109/MCOM.2014.6736761.

Lee, Kai-Fu. *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt, 2018.

Liao, Rita. “Huawei Says Two-Thirds of 5G Networks Outside China Now Use Its Gear.” *TechCrunch* (blog), June 25, 2019. http://social.techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

Lukhanyu, Milcah. “Huawei to Build Sh17.5b Konza Data Centre and Smart Cities Project.” *TechMoran*, April 27, 2019. https://techmoran.com/2019/04/27/huawei-bags-chinese-govt-deal-to-build-sh17-5b-konza-data-centre-and-smart-cities-project/.

Magnusson, Lars. *Mercantilism: The Shaping of an Economic Language*. New York: Routledge, 1994.

Maness, Ryan. “Chinese Cyber Behavior: Manipulation and Espionage.” Lecture. Monterey, CA: Naval Postgraduate School, November 7, 2019.

Marek, Sue. “Low-Band, Mid-Band or High-Band—Why Spectrum Bands Matter in a 5G World.” *Futurithmic*, February 11, 2020. https://www.futurithmic.com/2020/02/11/why-spectrum-bands-matter-in-a-5g-world/.

McFate, Sean. *The New Rules of War: Victory in the Age of Durable Disorder*. New York: William Morrow, 2019.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare: Theory & Practice*. Novato, CA: Presidio, 1995.

Medin, Milo, and Gilman Louie. *The 5G Ecosystem: Risks & Opportunities for DOD*. Defense Innovation Board, 2019.

"Mike Pompeo Urges Tories to Ask: 'What Would Thatcher Do?'" *The Guardian*, May 8, 2019, sec. Technology. https://www.theguardian.com/technology/2019/may/08/mike-pompeo-invokes-thatcher-push-harder-line-china-huawei.

Miracola, Sergio. "Chinese Hybrid Warfare." *Italian Institute for International Political Studies*, December 21, 2018. https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853.

Mishra, Yash. "Here Are the Countries That Allowed Huawei to Build 5G." *Huawei Central* (blog), August 30, 2019. https://www.huaweicentral.com/here-are-the-countries-that-allowed-huawei-to-build-5g-list/.

Moran, Theodore H. "An Economic Agenda for Neorealists." *International Security* 18 (2) (Fall 1993): 211–15.

Morris, Anne. "Ericsson Hails 5G Test on Another Sub-6 GHz Band." *SDxCentral*, January 14, 2019. https://www.sdxcentral.com/articles/news/ericsson-hails-5g-test-on-another-sub-6-ghz-band/2019/01/.

Mozur, Paul. "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras." *The New York Times*, July 8, 2018, sec. Business. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Mozur, Paul, and Aaron Krolik. "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers." *The New York Times*, December 17, 2019, sec. Technology. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html.

Nachemson, Andrew, and Kong Meta. "Cambodia's Digital Surveillance Is Silencing Government Critics." *Post Magazine*, October 19, 2019. https://www.scmp.com/magazines/post-magazine/long-reads/article/3033508/cambodias-digital-surveillance-serves-silence.

Norton. "What Are Cookies?" Norton, 2020. https://us.norton.com/internetsecurity-how-to-what-are-cookies.html.

Okimoto, Daniel. *Between MITI and the Market: Japanese Industrial Policy for High Technology*. Stanford: Stanford University Press, 1990.

Orchard, Phillip. “China’s Plan to Win Over Cambodia.” *Real Clear*, August 1, 2019, sec. World. https://www.realclearworld.com/articles/2019/08/01/chinas_plan_to_win_over_cambodia_113068.html.

Parkinson, Joe, Nicholas Bariyo, and Josh Chin. “Huawei Technicians Helped African Governments Spy on Political Opponents.” *The Wall Street Journal*. August 15, 2019, sec. Tech. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

“Public Policy Position: 5G Spectrum.” Huawei, 2017. https://www-file.huawei.com/-/media/CORPORATE/PDF/public-policy/public_policy_position_5g_spectrum.pdf.

Qualcomm. “How 5G Massive MIMO Transforms Your Mobile Experiences,” June 20, 2019. https://www.qualcomm.com/news/onq/2019/06/20/how-5g-massive-mimo-transforms-your-mobile-experiences.

———. “Key Breakthroughs to Drive a Fast and Smooth Transition to 5G Standalone,” August 2, 2019. https://www.qualcomm.com/news/onq/2019/08/19/key-breakthroughs-drive-fast-and-smooth-transition-5g-standalone.

“Radio-Frequency Spectrum.” In *Encyclopedia Britannica*, 2013. https://www.britannica.com/science/radio-frequency-spectrum.

RF Wireless World. “Difference Between 4G and 5G.” Accessed February 7, 2020. https://www.rfwireless-world.com/Terminology/4G-vs-5G-difference-between-4G-and-5G.html.

Rothstein, Hy, and Barton Whaley. *The Art and Science of Military Deception*. Boston: Artech House, 2013.

Segan, Sascha. “T-Mobile Announces 5G in 6 Cities: We Have the Maps.” *PCMagazine*, June 25, 2019. https://www.pcmag.com/news/t-mobile-announces-5g-in-6-cities-we-have-the-maps.

Singer, P. W., and Emerson T. Brooking. “Social Media Is Revolutionizing Warfare.” *The Atlantic*, October 2, 2018, sec. Global. https://www.theatlantic.com/international/archive/2018/10/likewar-internet-new-intelligence-age-flynn/571903/.

Sunny Classroom. “5G Cellular Networks: 6 New Technologies.” Video, 11:57, December 7, 2018. https://www.youtube.com/watch?v=hQvHNVRv_ms.

Sutton, Gordon J., Jie Zeng, Ren Ping Liu, Wei Ni, Diep N. Nguyen, Beeshanga A. Jayawickrama, Xiaojing Huang et al. “Enabling Technologies for Ultra-Reliable and Low Latency Communications: From PHY and MAC Layer Perspectives.” *IEEE Communications Surveys Tutorials* 21, no. 3 (Third Quarter 2019): 2488–2524. https://doi.org/10.1109/COMST.2019.2897800.

Thul, Prak Chan. “Cambodia Kicks Off Drills with ‘Great Friend’ China as U.S. Ties Sour.” *Reuters*, March 17, 2018, sec. World News. https://www.reuters.com/article/us-cambodia-china-military-idUSKCN1GT05F.

———. “Cambodia PM Dismisses Fears of Chinese Debt Trap.” *Reuters*, May 30, 2019, sec. World News. https://www.reuters.com/article/us-cambodia-china-idUSKCN1T00U8.

T-Mobile. “Built for the 5G Future: T-Mobile Opens New Device Lab,” August 20, 2019. https://www.t-mobile.com/news/5g-device-lab.

Turton, Shaun, and Tomoya Onishi. “Cambodia 5G Set to Leapfrog ASEAN Rivals with Huawei and ZTE.” *Nikkei Asian Review*, September 5, 2019. https://asia.nikkei.com/Spotlight/5G-networks/Cambodia-5G-set-to-leapfrog-ASEAN-rivals-with-Huawei-and-ZTE.

Underwood, Kimberly. “5G for Warfighters.” *SIGNAL Magazine*, June 1, 2019. https://www.afcea.org/content/5g-warfighters.

Villas-Boas, Antonio, and Lisa Eadicicco. “Why Huawei Smartphones Are Popular All Over the World, Except the US.” *Business Insider*, May 20, 2019. https://www.businessinsider.com/huawei-smartphones-are-popular-all-over-world-not-united-states-2018-12.

Watts, John T. “A Framework for an Open, Trusted, and Resilient 5G Global Telecommunications Network.” *Atlantic Council*, March 2020. https://www.atlanticcouncil.org/wp-content/uploads/2020/03/Framework-for-a-5G-Network.pdf.

Whaley, Barton. “Chapter 44: Lessons from Behind Other Hills: Planning Deceptions in 145 Different Disciplines.” In *The Art and Science of Military Deception*. Boston: Artech House, 2007.

Wheeler, Tom, and David Simpson. “Why 5G Requires New Approaches to Cybersecurity.” *Brookings*, September 3, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

Wheeler, Tom, and Robert D. Williams. “Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G.” In *Huawei, 5G and National Security: A Lawfare Compilation*. Washington, DC: Lawfare Institute, 2019. www.lawfareblog.com.

White House, The. *National Strategy to Secure 5G of the United States of America*. Washington, DC: The White House, 2020. https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Wright, Nicholas. “How Artificial Intelligence Will Reshape the Global Order,” October 11, 2019. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order.

Yap, Chuin-Wei. “State Support Helped Fuel Huawei’s Global Rise.” *Wall Street Journal*, December 25, 2019, sec. Tech. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

Zuboff, Shoshana. “‘Surveillance Capitalism’ Has Gone Rogue. We Must Curb Its Excesses.” *The Washington Post*. January 24, 2019, sec. Opinion.

———. “You Are Now Remotely Controlled.” *The New York Times*, January 24, 2020, sec. Opinion. https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California